Université de Technologie Haïti

Faculté des Sciences Informatiques

TD 2

Préparé par

Jean Saint Louis Joseph VALMY

Cours

Cybersécurité

Professeur

Ismaël SAINT AMOUR

Niveau

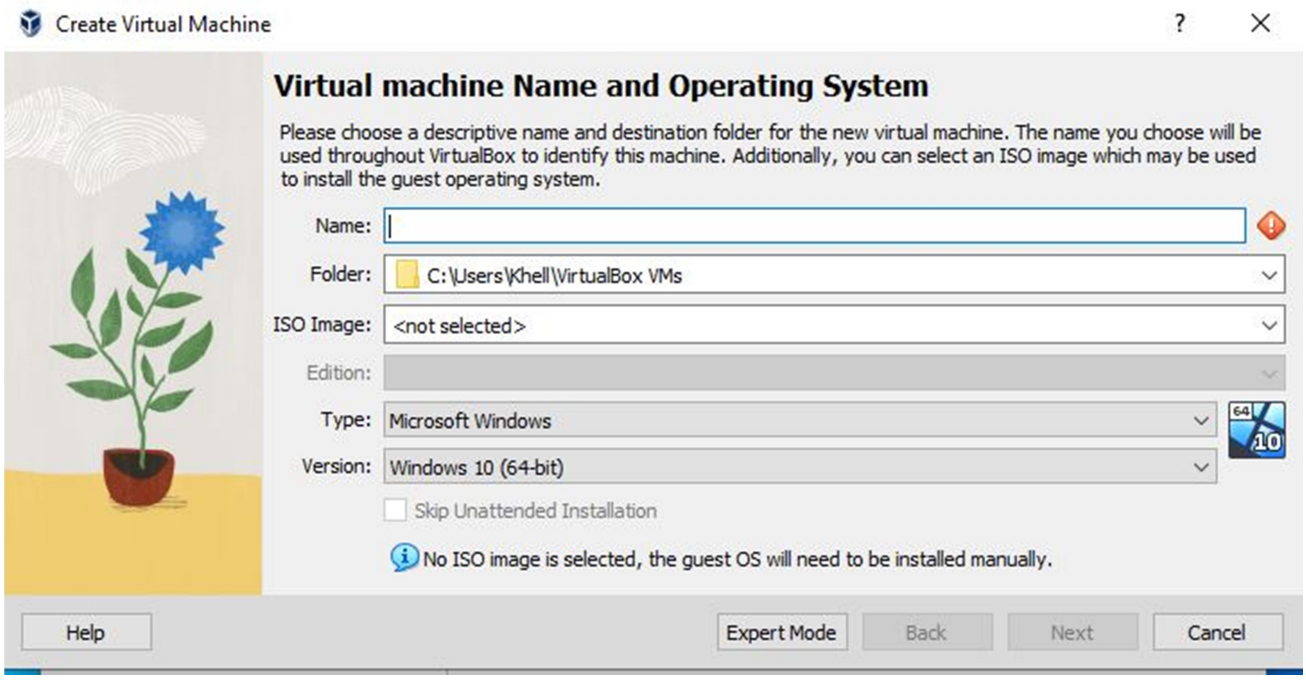
4e Année

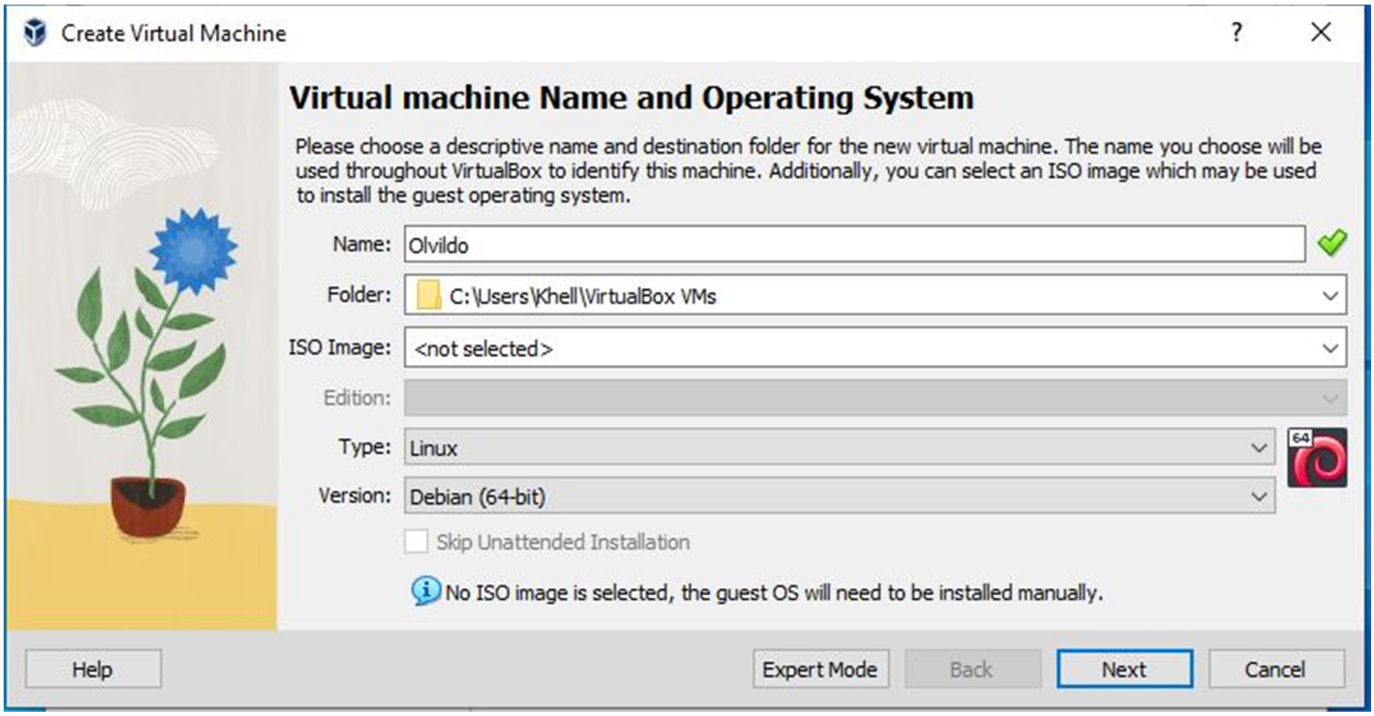
Port-au-Prince, le 11 février 2025

1. Création et configuration de la machine virtuelle dans virtualBox

- Interface de la machine virtuelle Virtual Box

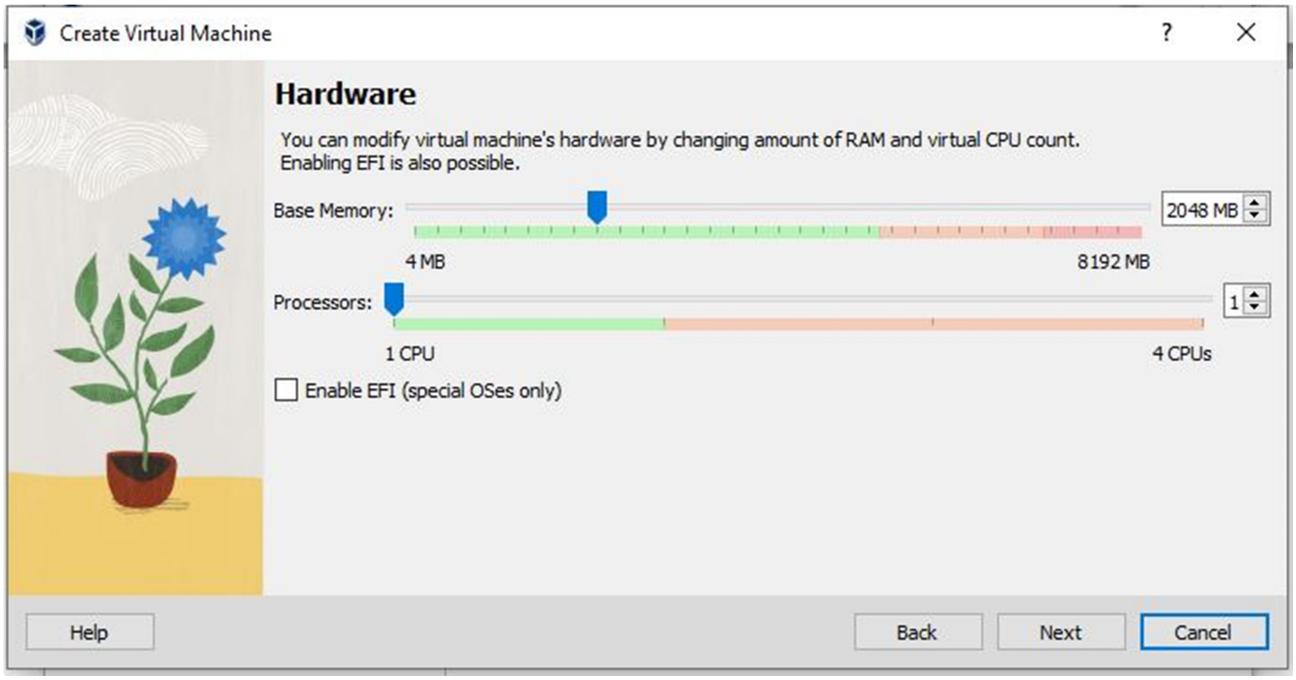
Virtual Box est lancée





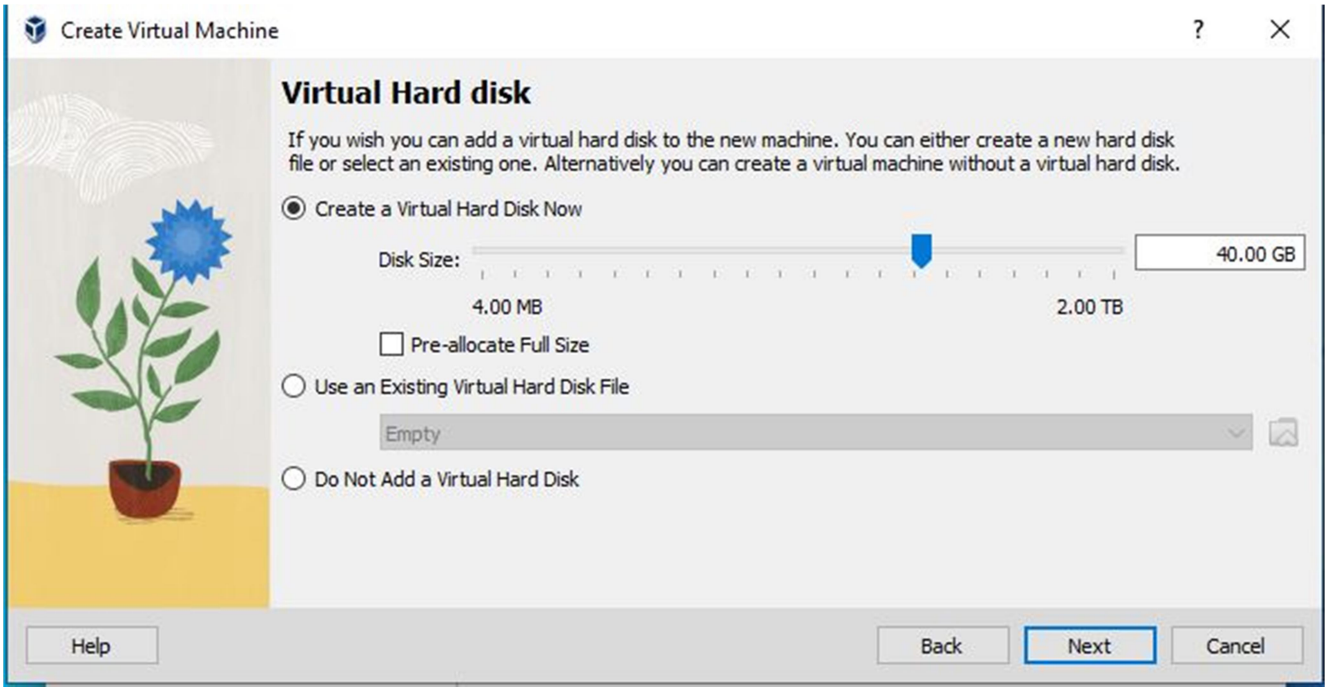
Le nom “Olvildo”, le type “Linux” et la version “Debian (64-bit)” ont été attribués à la machine virtuelle.

- Assignation de la mémoire RAM

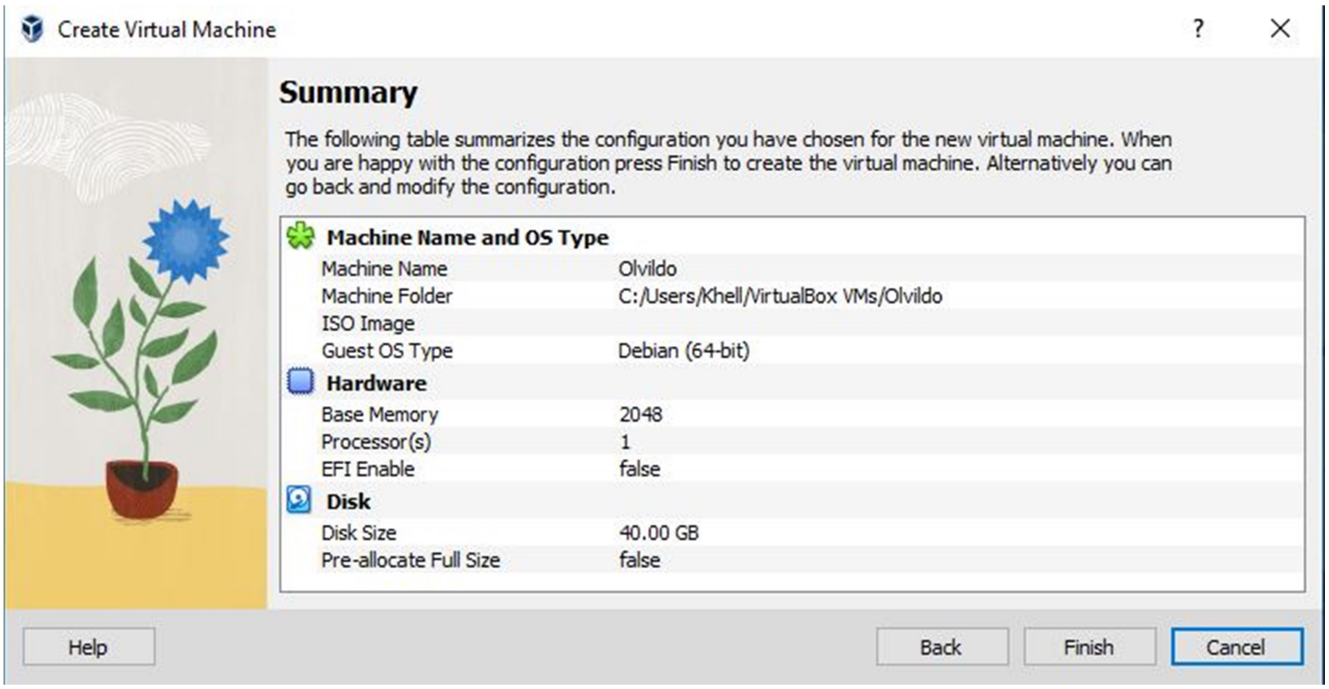


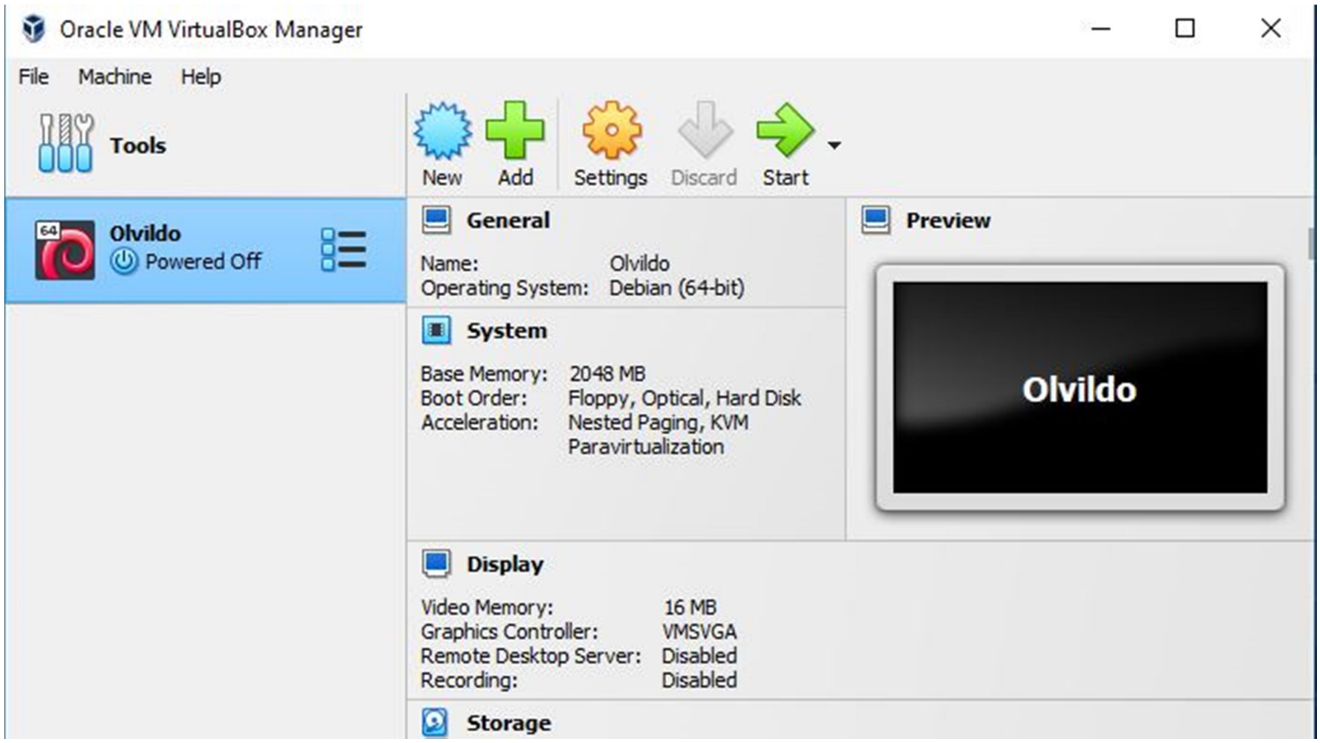
La quantité de mémoire qui est assignée à la machine est 2048 Mo

- Attribution de la taille du disque dur

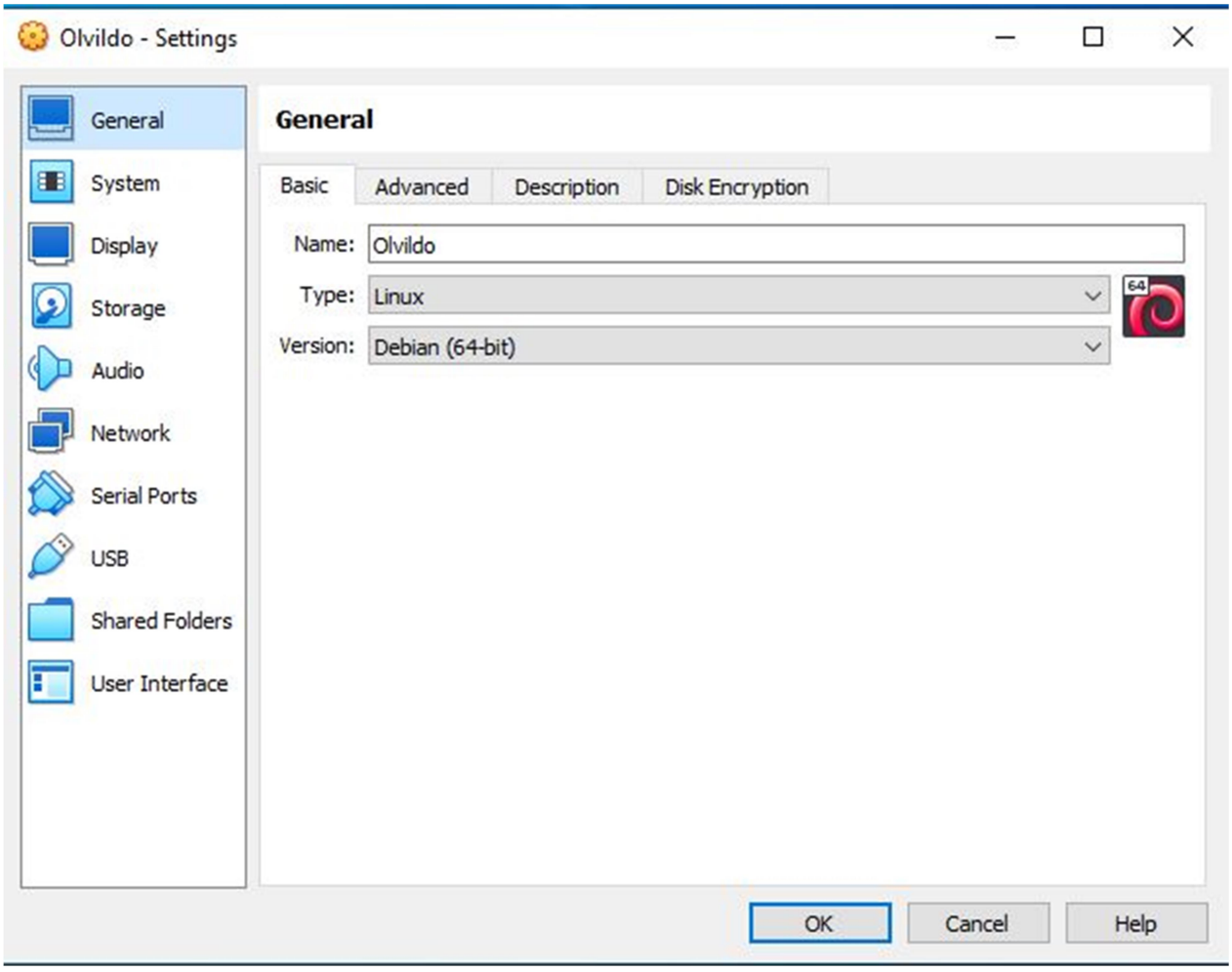


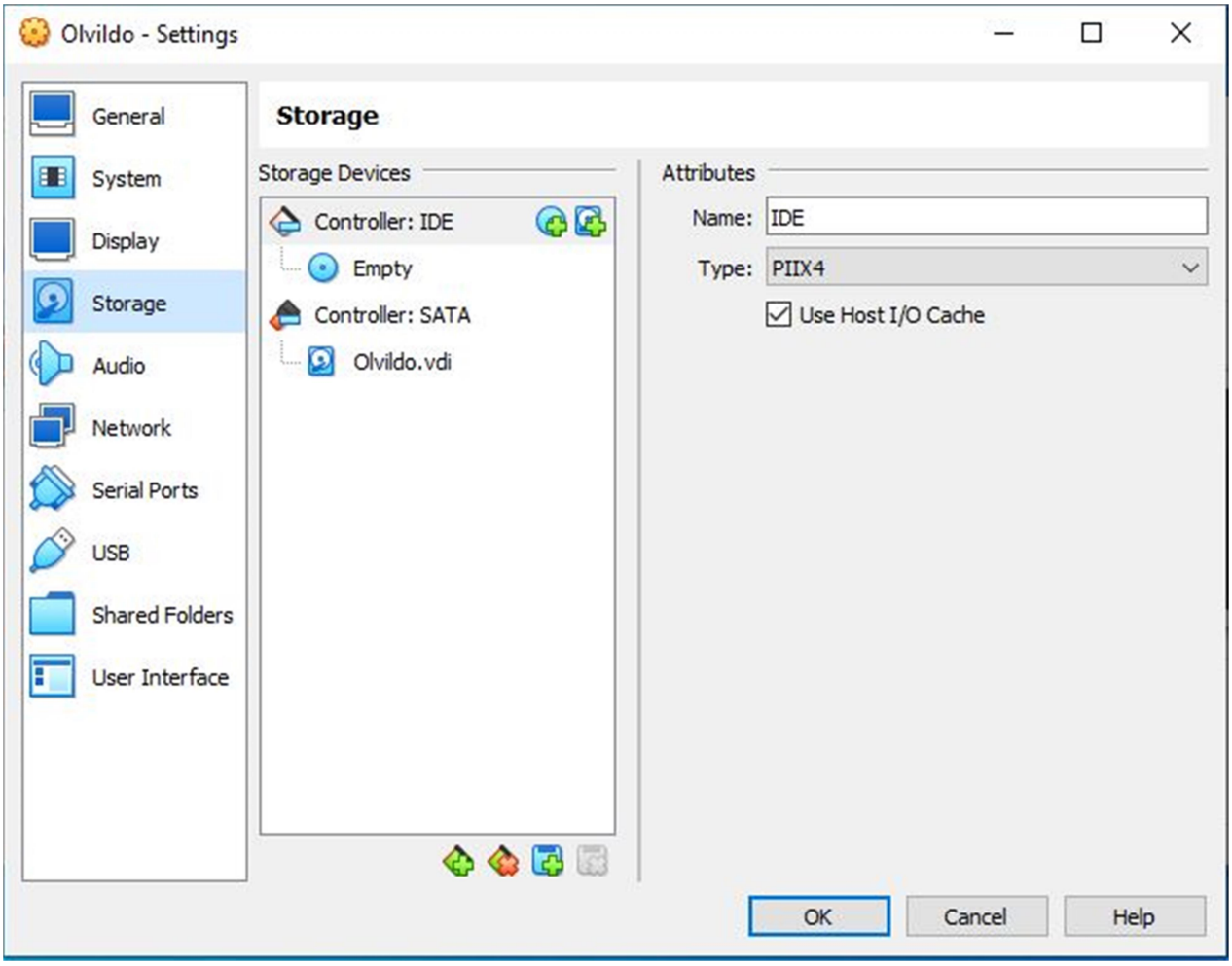
La taille du disque dur qui est alloué à la machine virtuelle est 40GB.

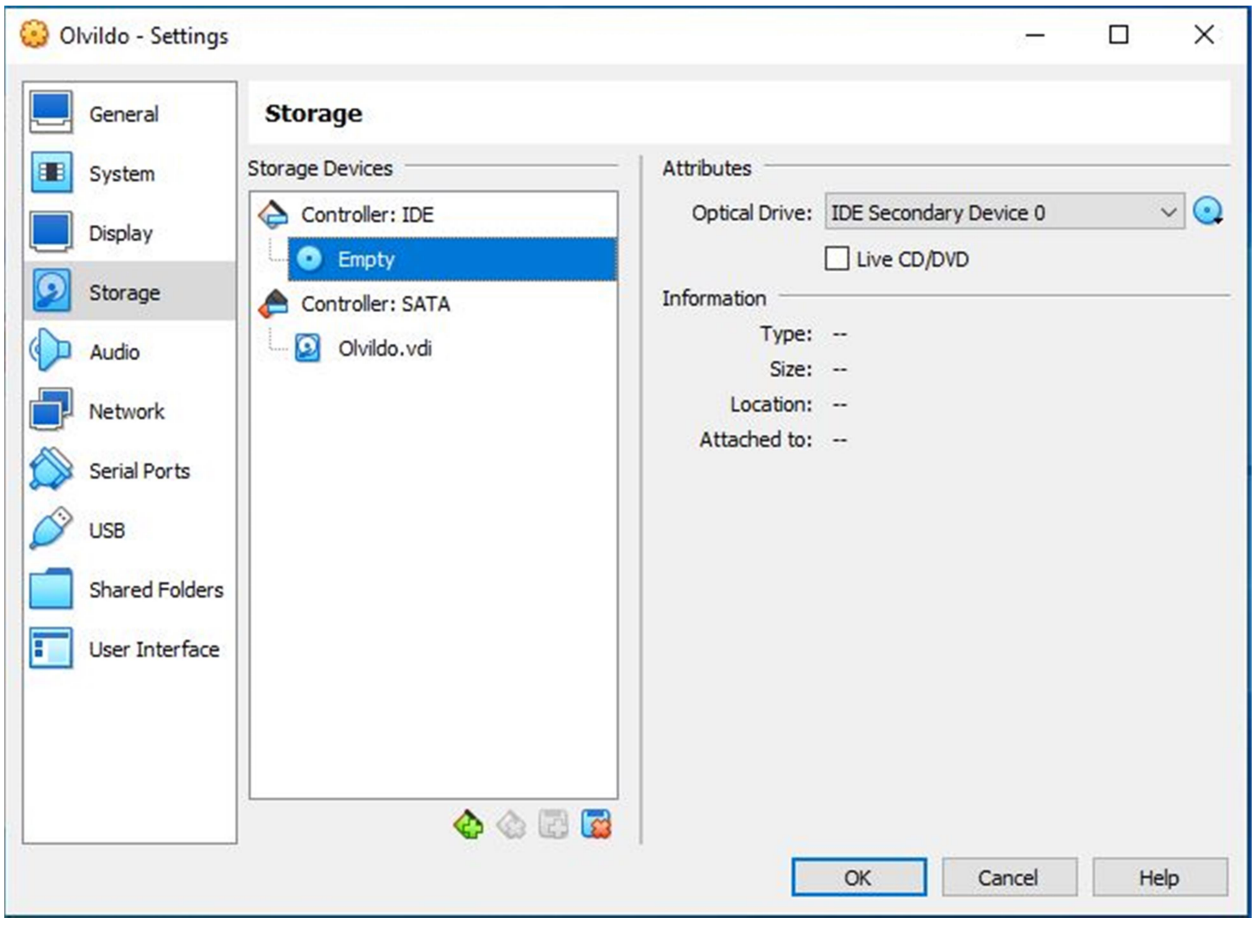


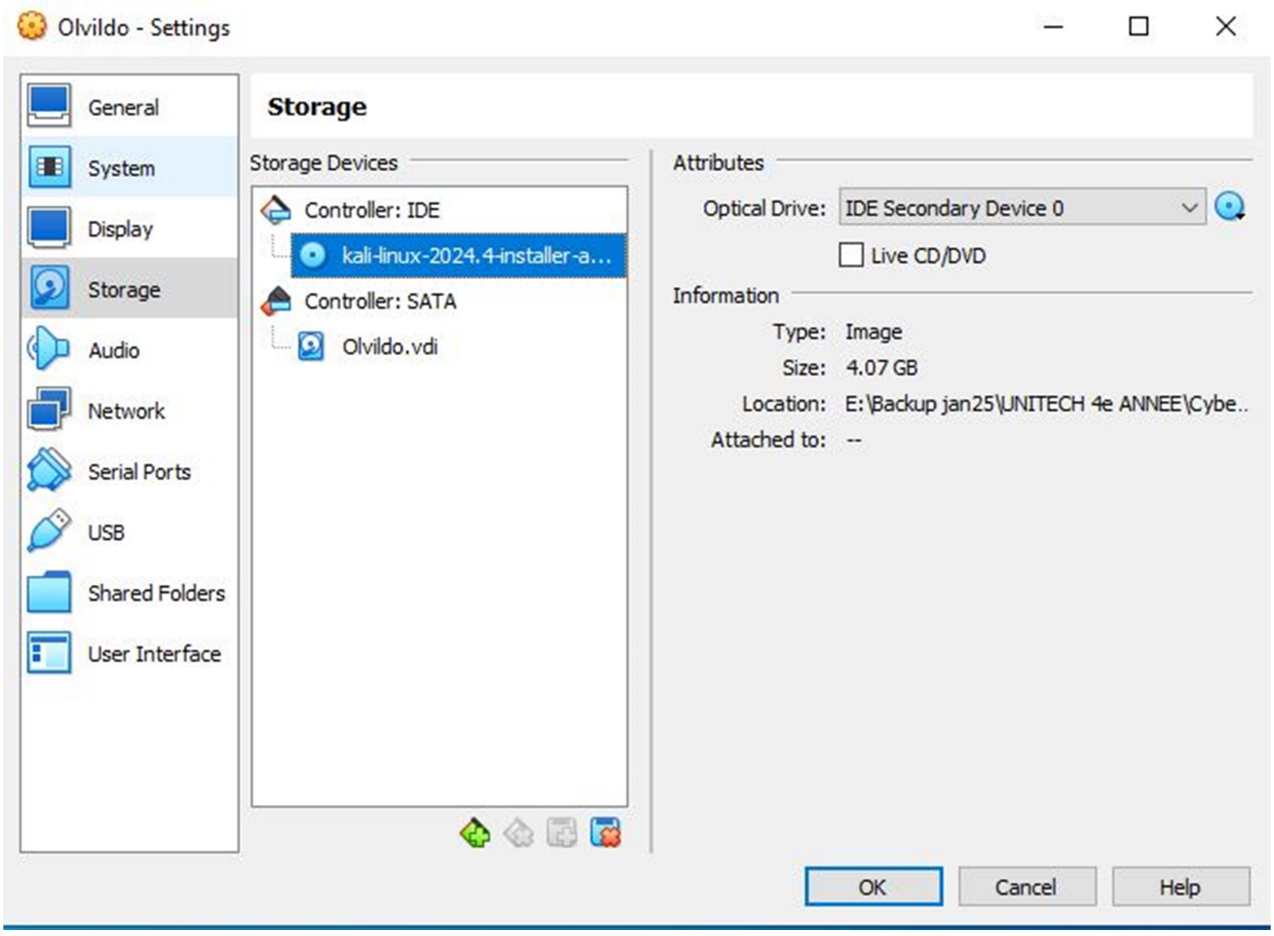


- Montage de l'image ISO



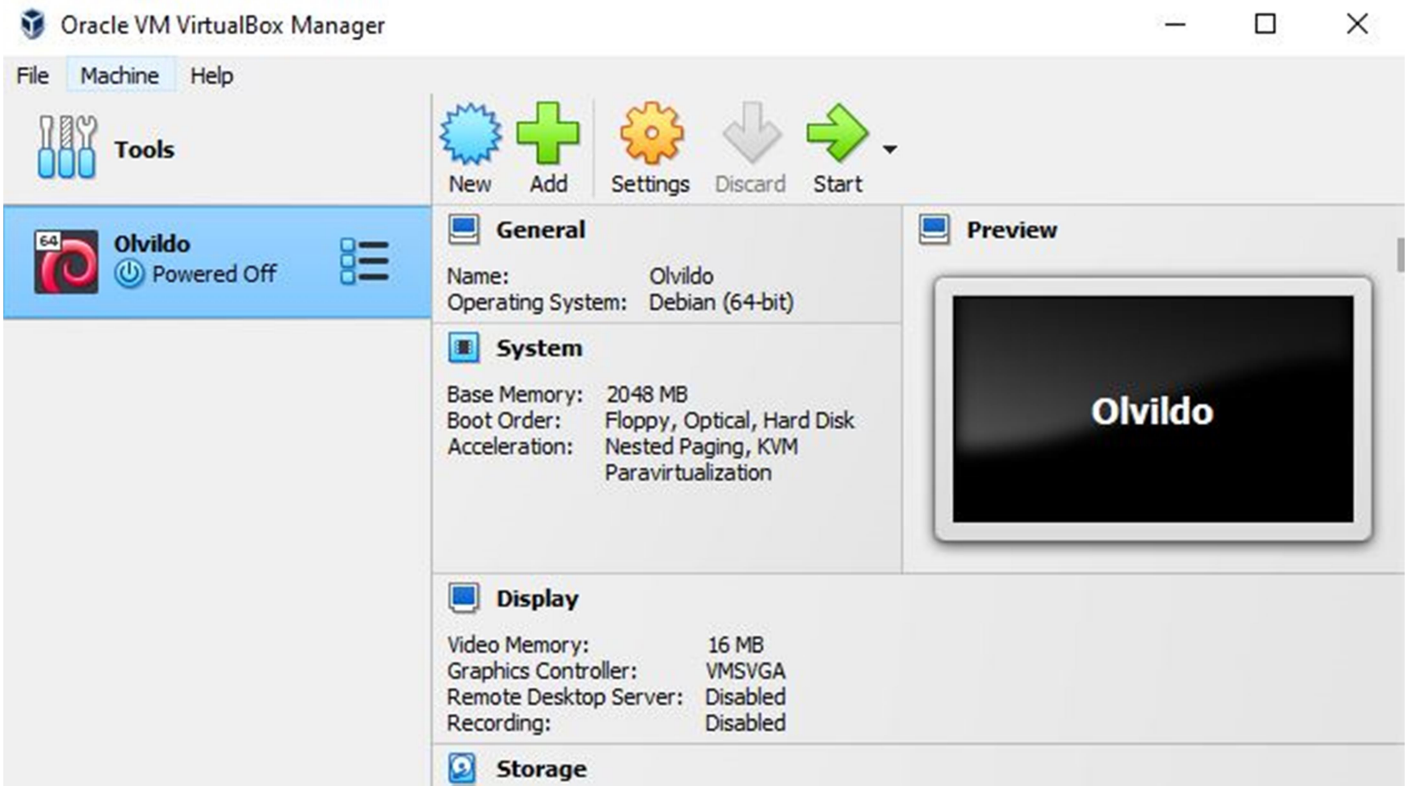

Olvildo - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Devices
Controller: IDE
Empty
Controller: SATA
Olvildo.vdi
Attributes
Name: IDE
Type: PIIX4
Use Host I/O Cache
OK
Cancel
Help

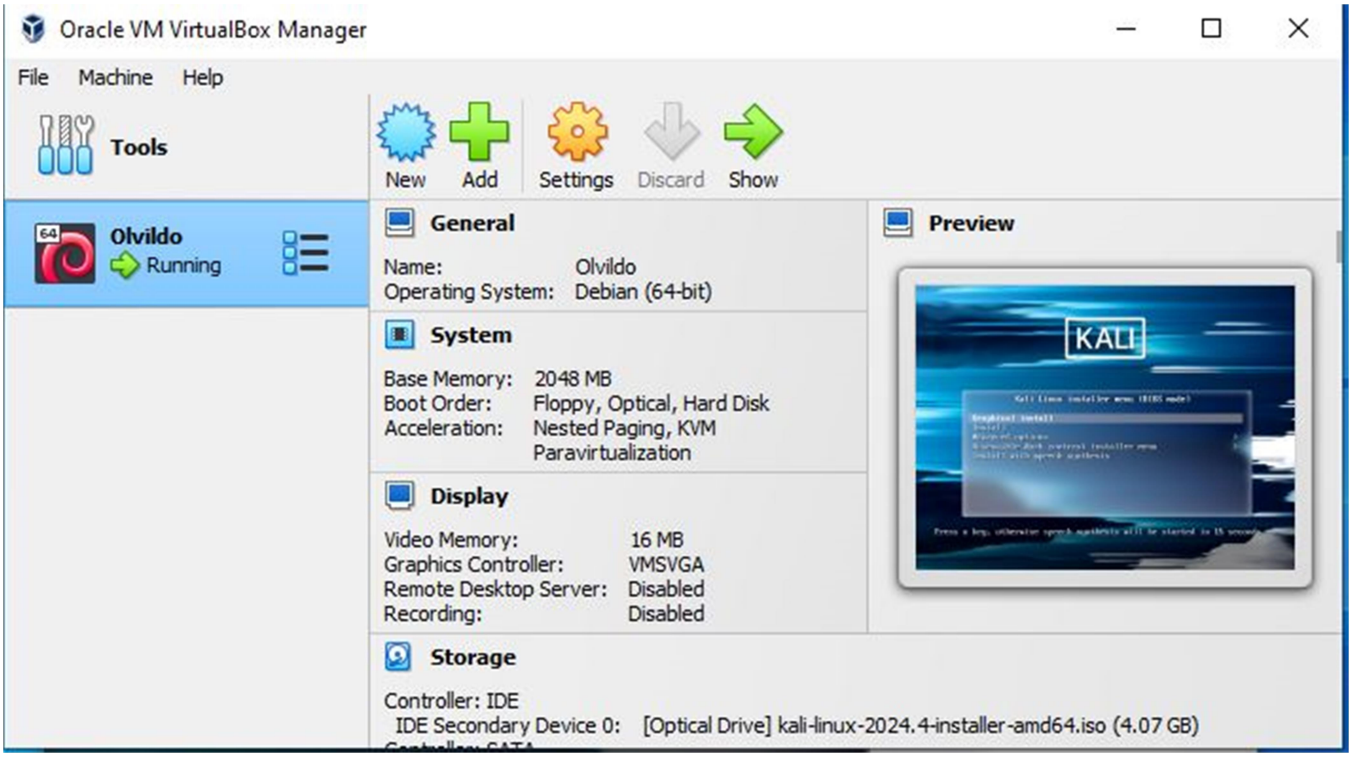

Olvildo - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Devices
Controller: IDE
Empty
Controller: SATA
Olvildo.vdi
Attributes
Optical Drive: IDE Secondary Device 0
Live CD/DVD
Information
Type: --
Size: --
Location: --
Attached to: --
OK
Cancel
Help



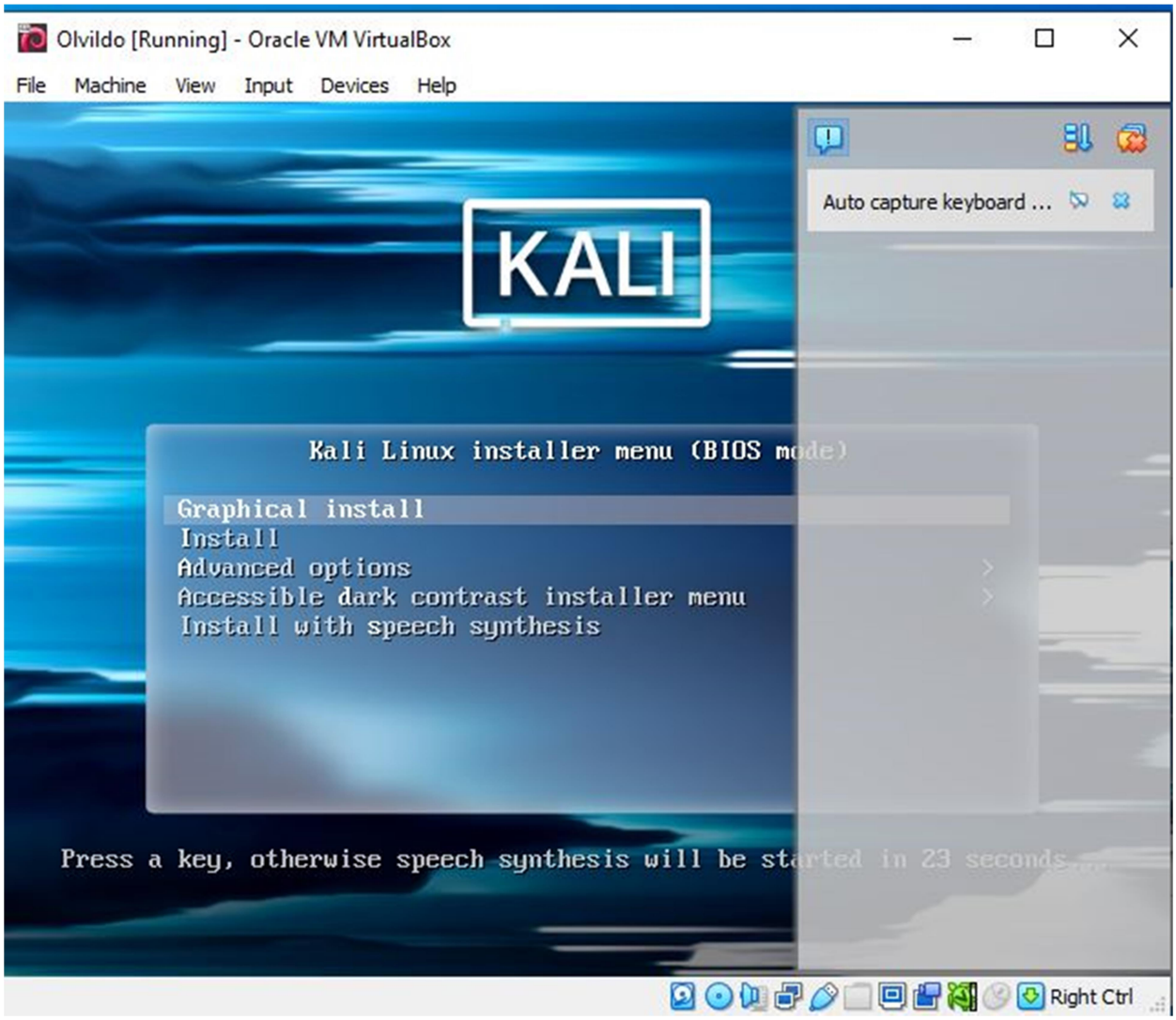
L'image ISO est sélectionnée comme périphérique de démarrage

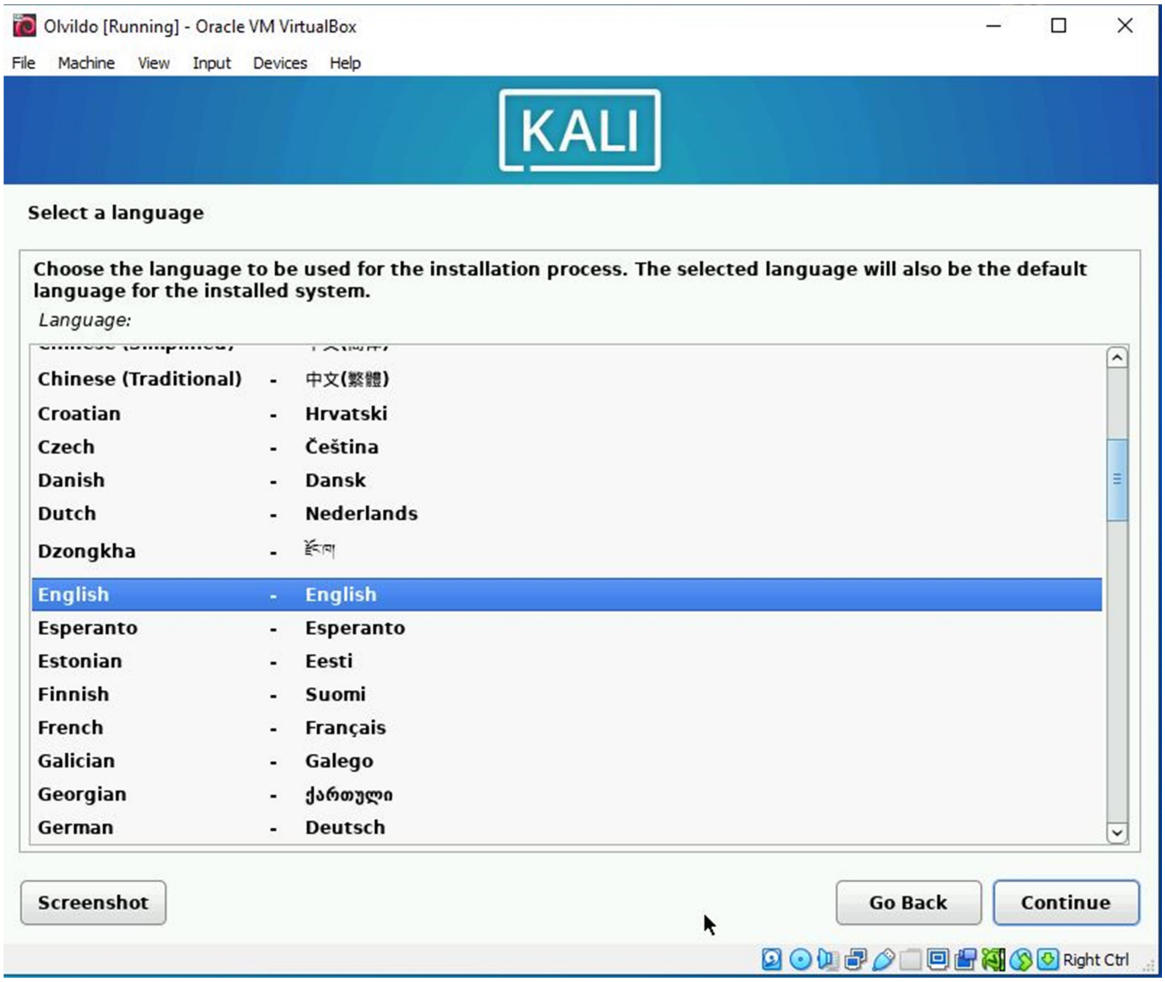
- Lancement de la machine virtuelle

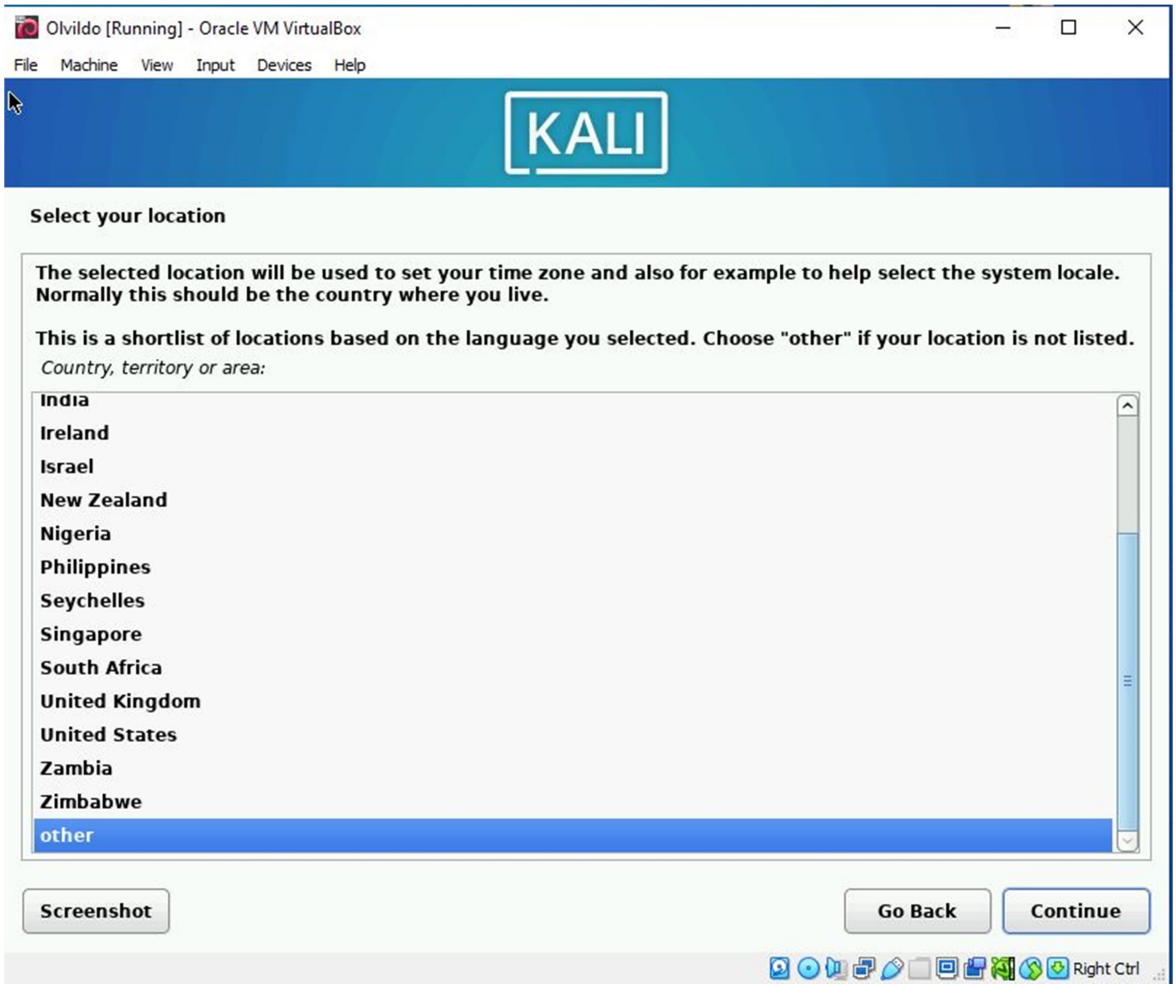


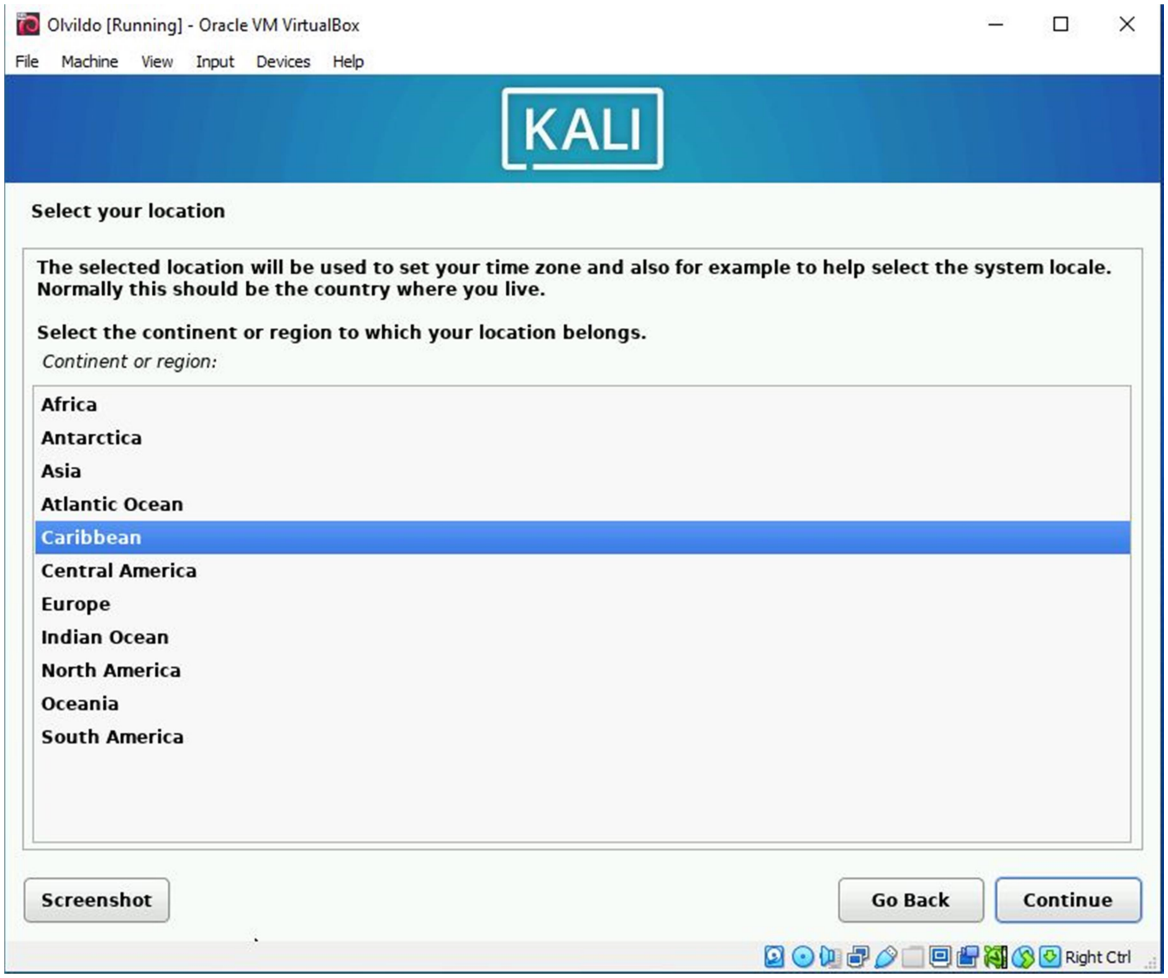


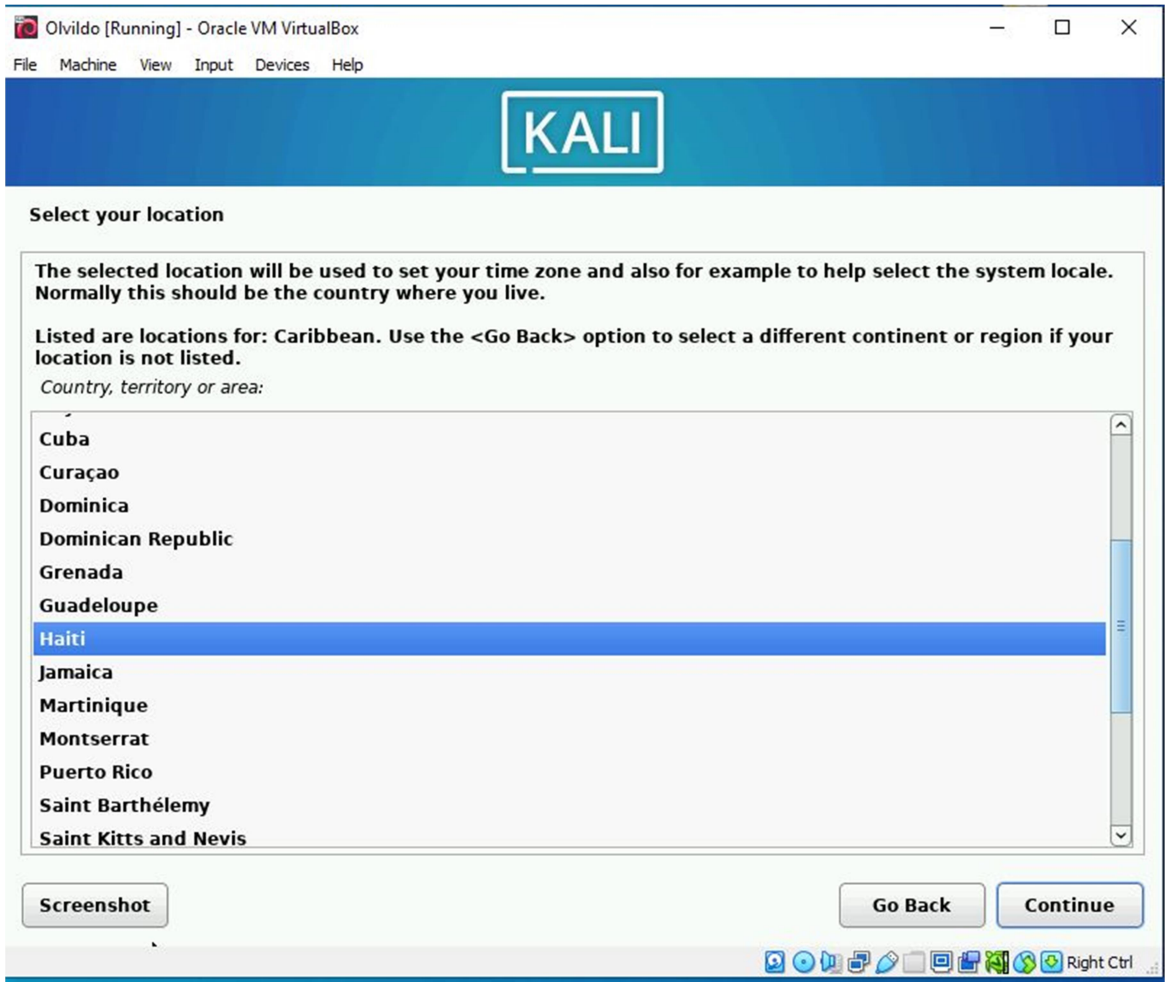
2. Installation de Kali Linux

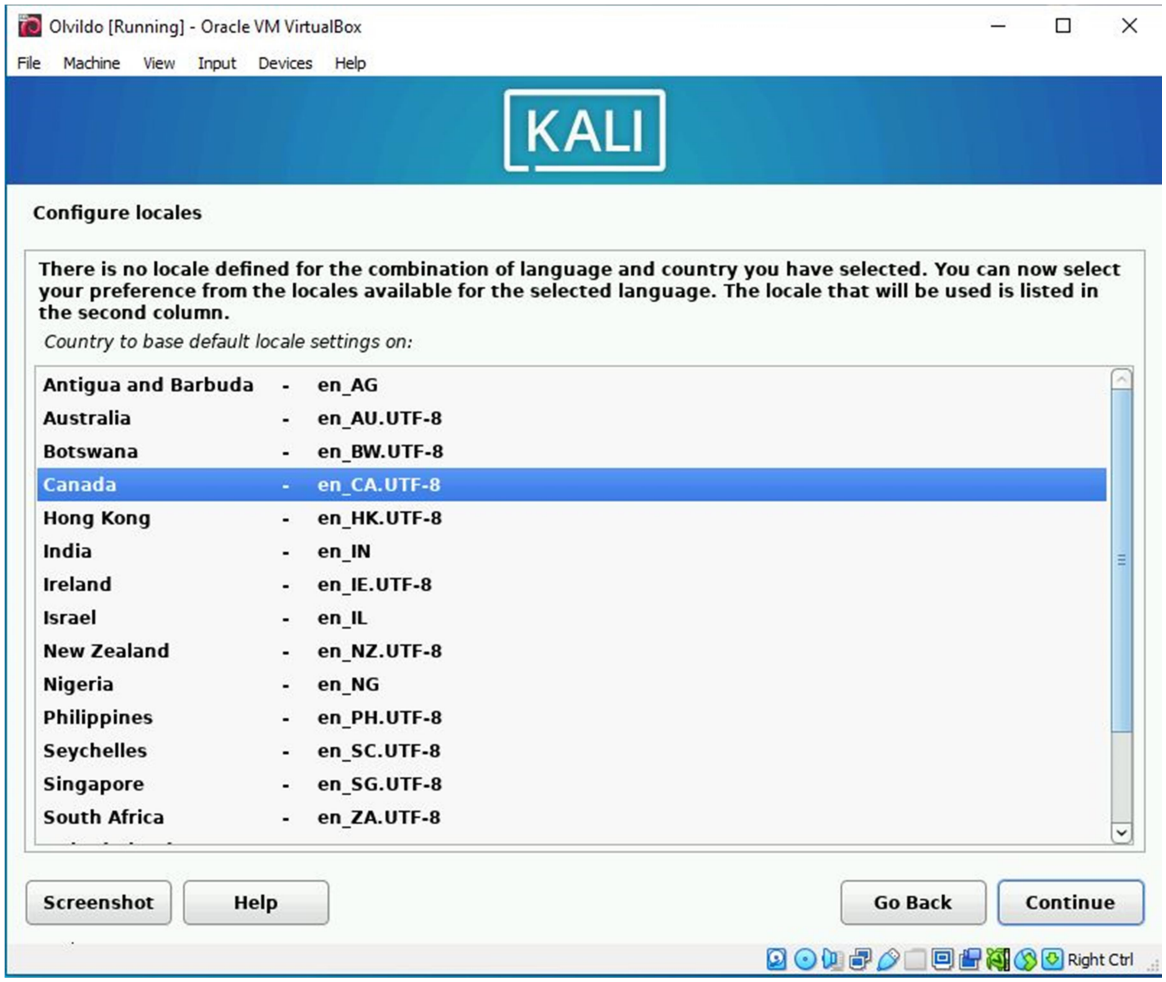


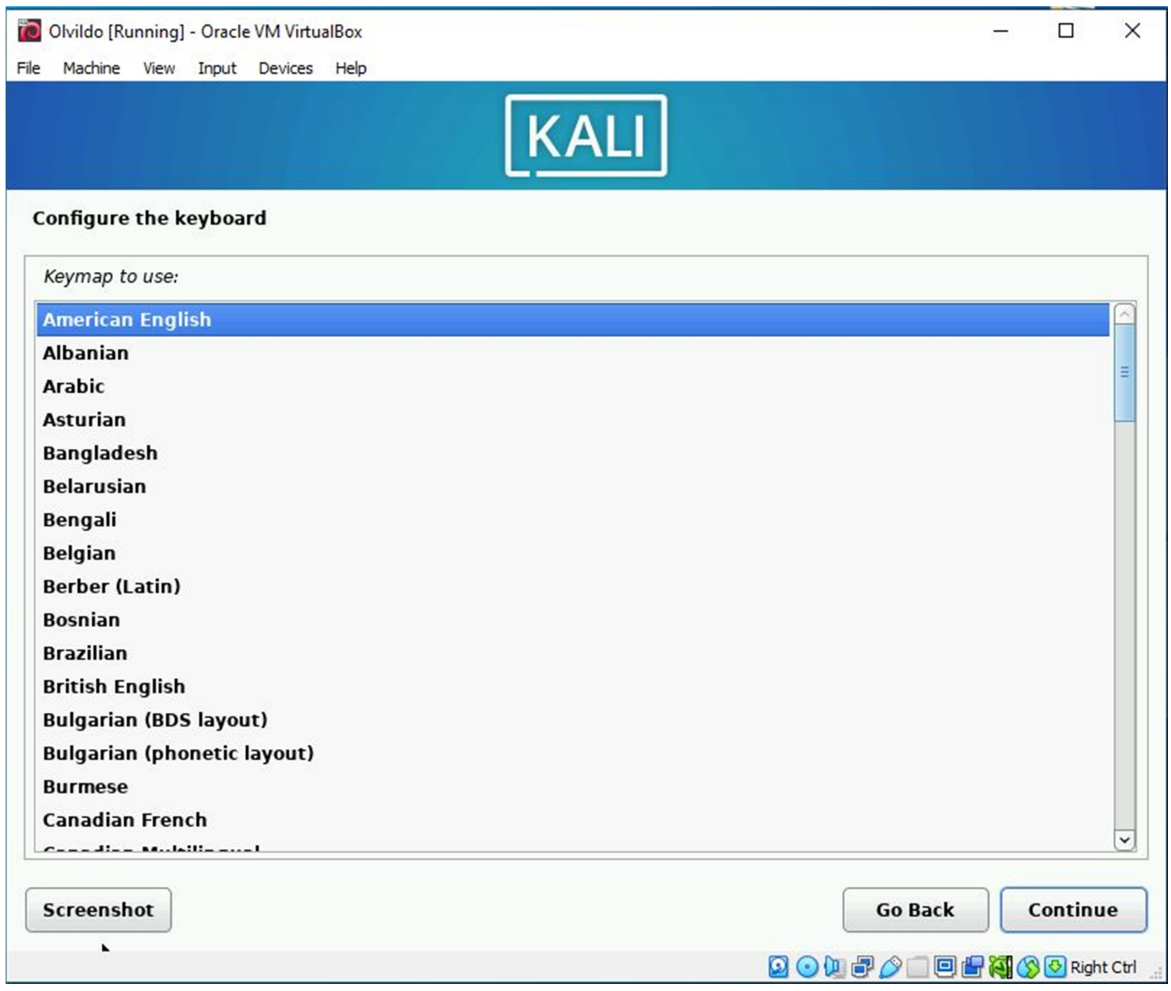

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
Dzongkha - རྫོང་ཁ
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
Screenshot
Go Back
Continue
Right Ctrl

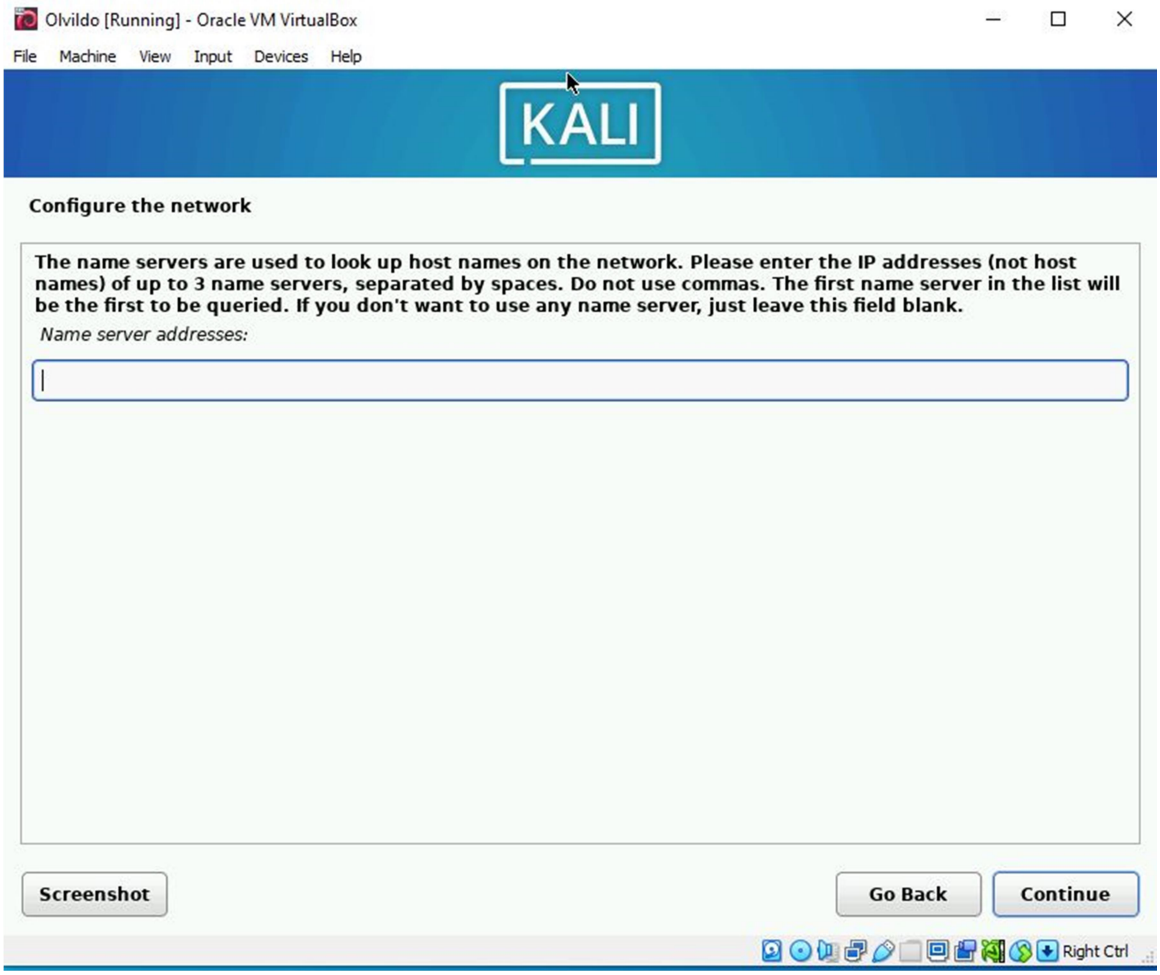

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
Screenshot
Go Back
Continue
Right Ctrl

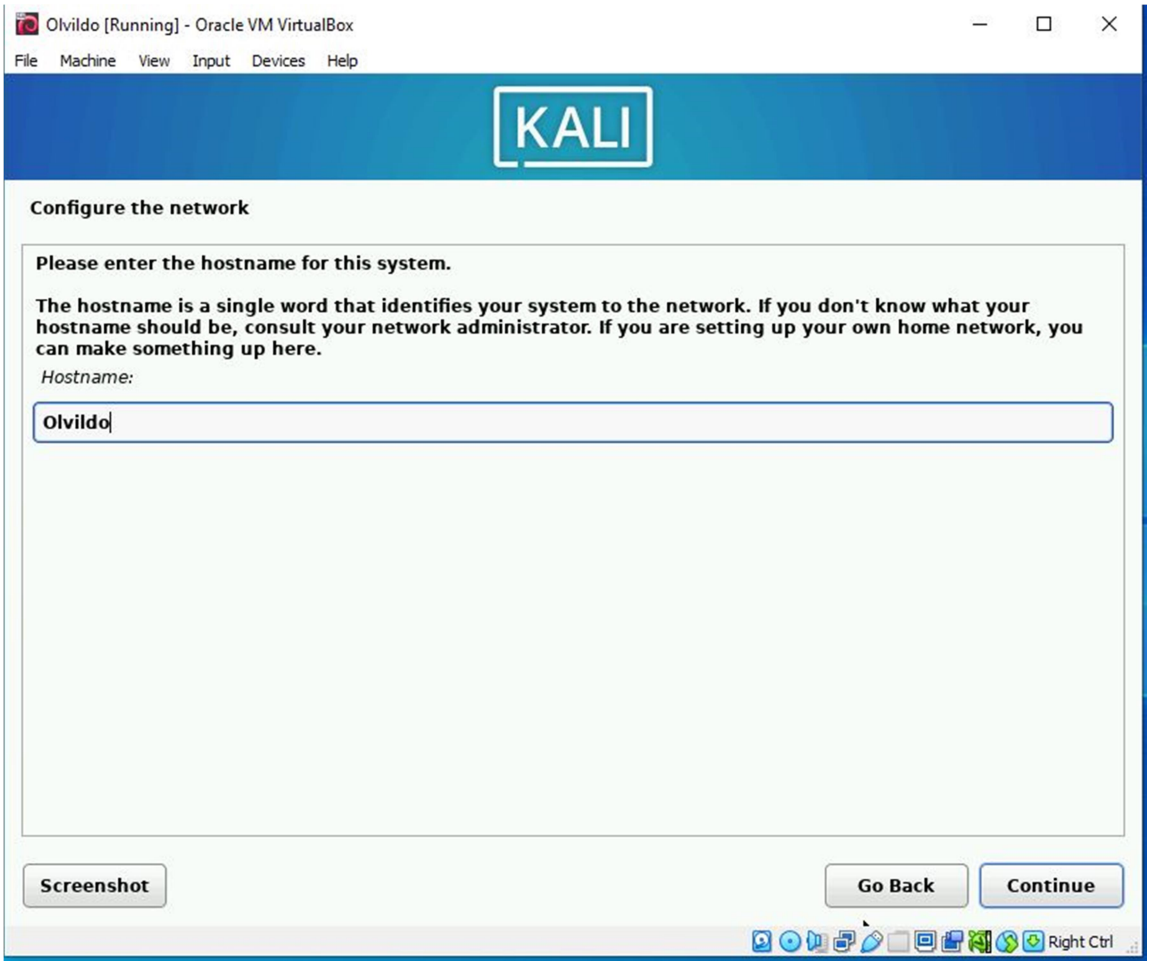

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
Select the continent or region to which your location belongs.
Continent or region:
Africa
Antarctica
Asia
Atlantic Ocean
Caribbean
Central America
Europe
Indian Ocean
North America
Oceania
South America
Screenshot
Go Back
Continue
Right Ctrl

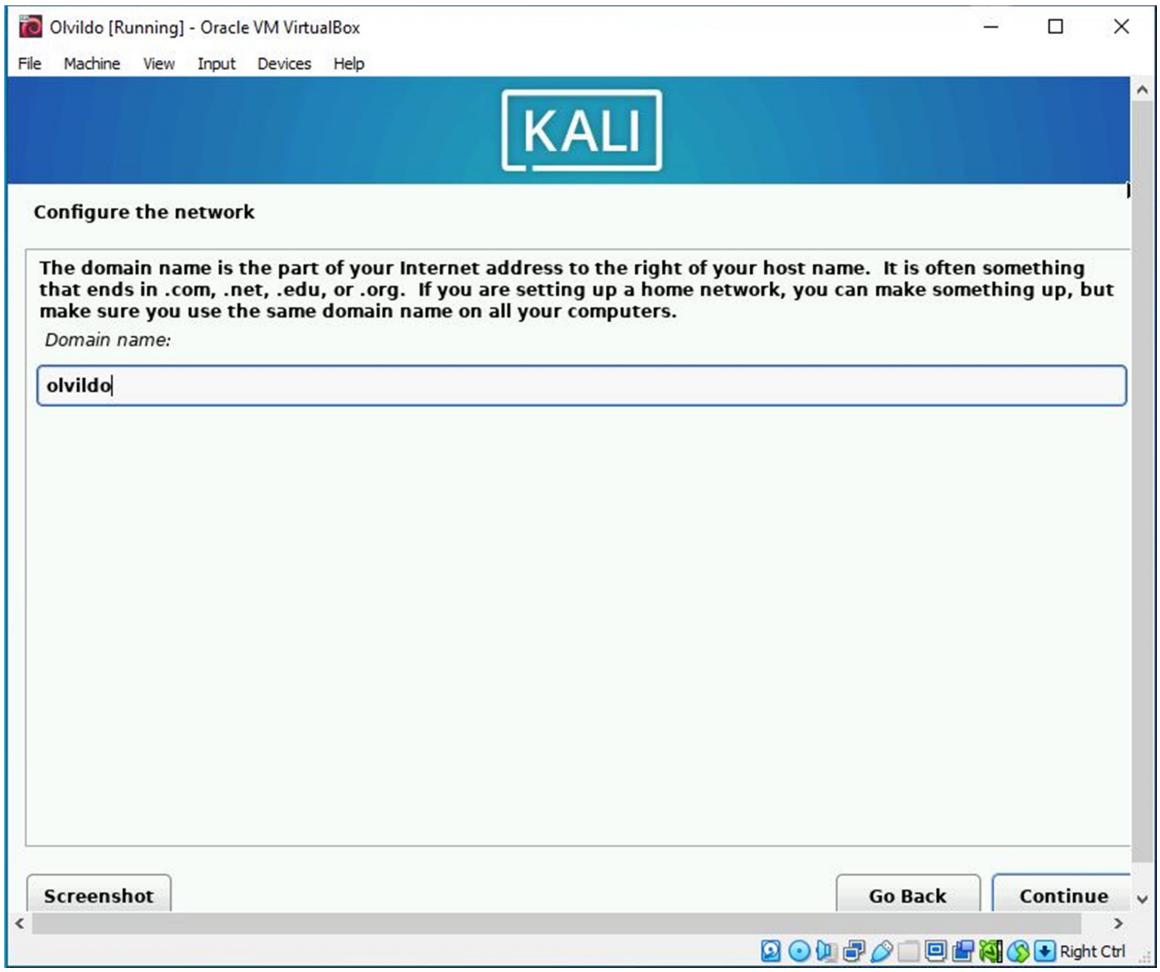

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
Listed are locations for: Caribbean. Use the <Go Back> option to select a different continent or region if your location is not listed.
Country, territory or area:
Cuba
Curaçao
Dominica
Dominican Republic
Grenada
Guadeloupe
Haiti
Jamaica
Martinique
Montserrat
Puerto Rico
Saint Barthélemy
Saint Kitts and Nevis
Screenshot
Go Back
Continue
Right Ctrl

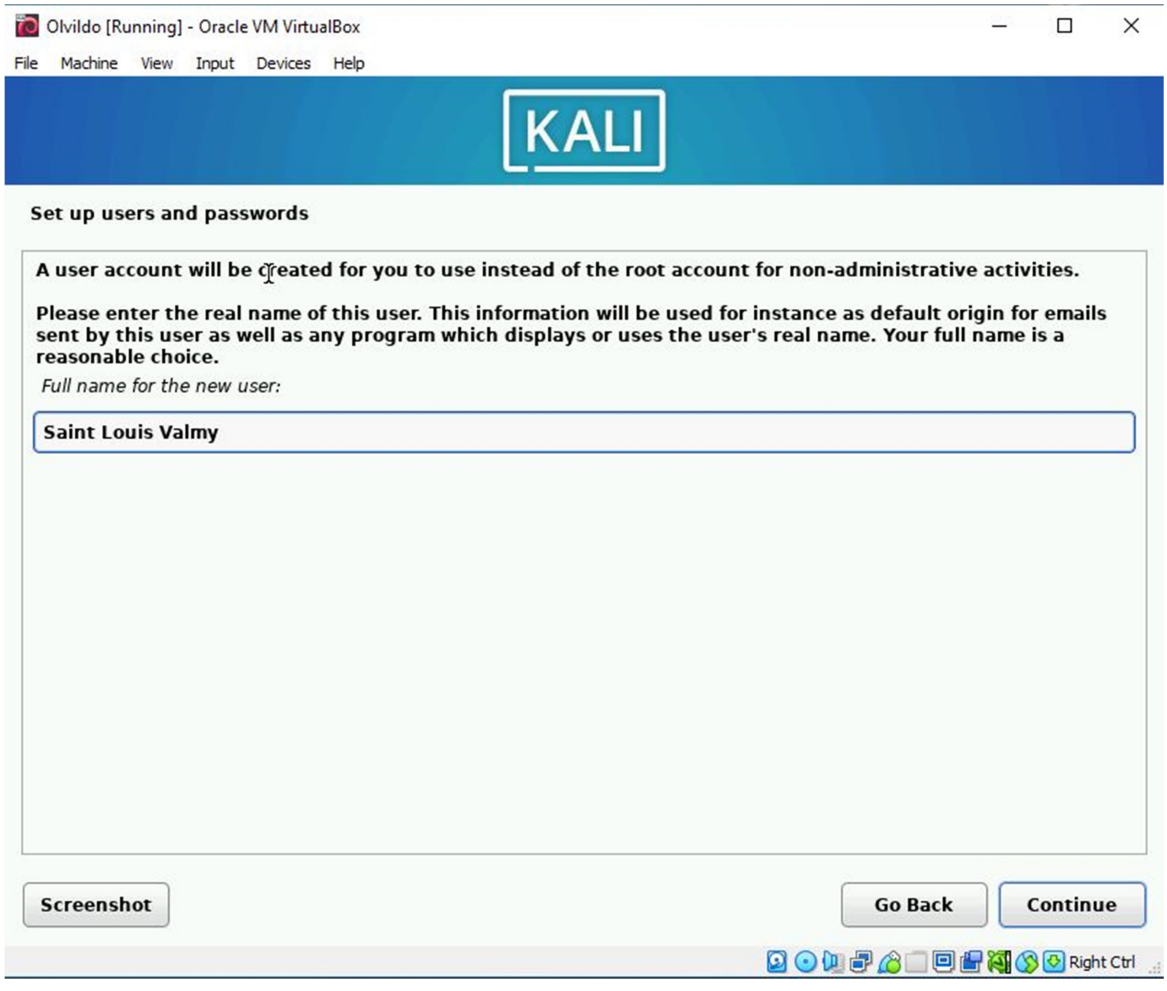

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Configure locales
There is no locale defined for the combination of language and country you have selected. You can now select your preference from the locales available for the selected language. The locale that will be used is listed in the second column.
Country to base default locale settings on:
Antigua and Barbuda - en_AG
Australia - en_AU.UTF-8
Botswana - en_BW.UTF-8
Canada - en_CA.UTF-8
Hong Kong - en_HK.UTF-8
India - en_IN
Ireland - en_IE.UTF-8
Israel - en_IL
New Zealand - en_NZ.UTF-8
Nigeria - en_NG
Philippines - en_PH.UTF-8
Seychelles - en_SC.UTF-8
Singapore - en_SG.UTF-8
South Africa - en_ZA.UTF-8
Screenshot
Help
Go Back
Continue
Right Ctrl

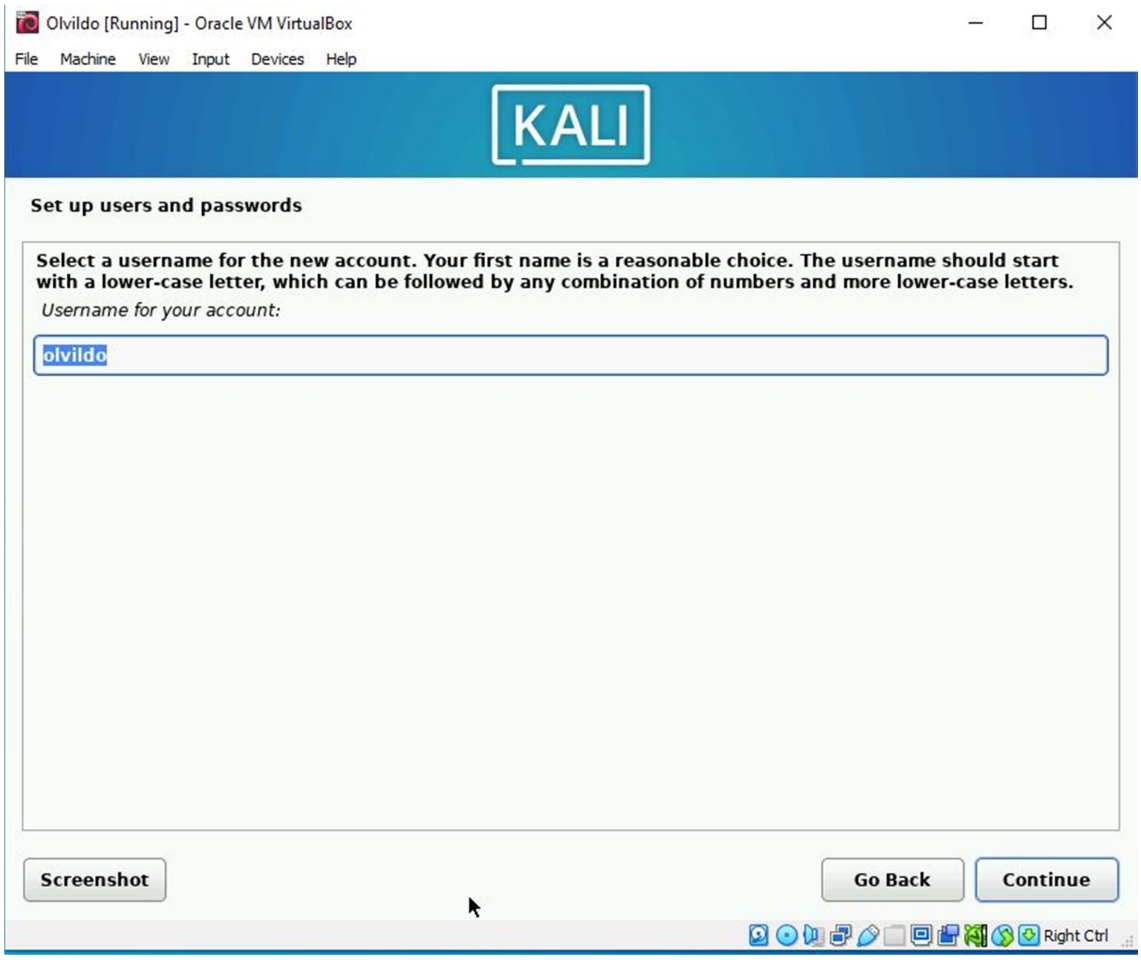

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Configure the keyboard
Keymap to use:
American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Berber (Latin)
Bosnian
Brazilian
British English
Bulgarian (BDS layout)
Bulgarian (phonetic layout)
Burmese
Canadian French
Screenshot
Go Back
Continue
Right Ctrl

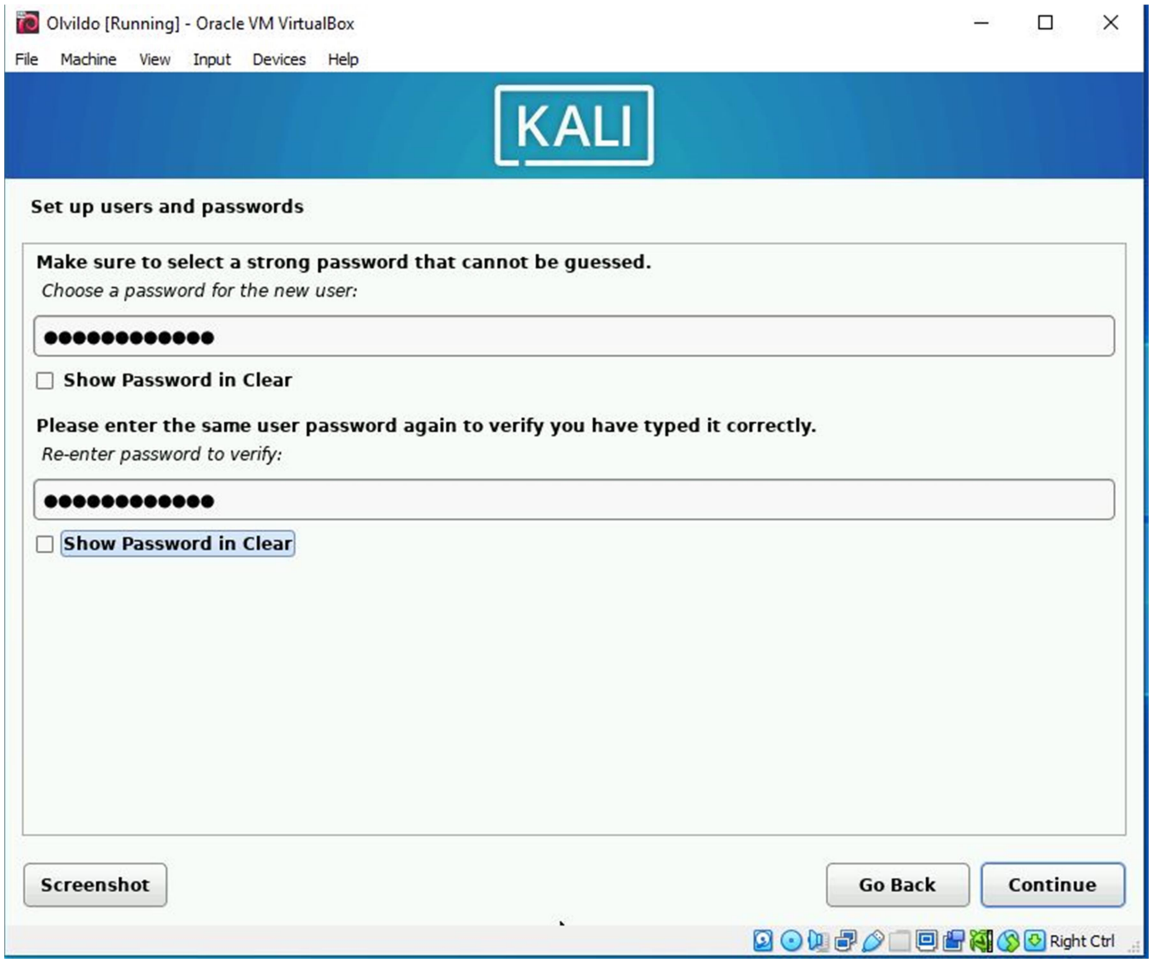

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Configure the network
The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.
Name server addresses:
Screenshot
Go Back
Continue
Right Ctrl

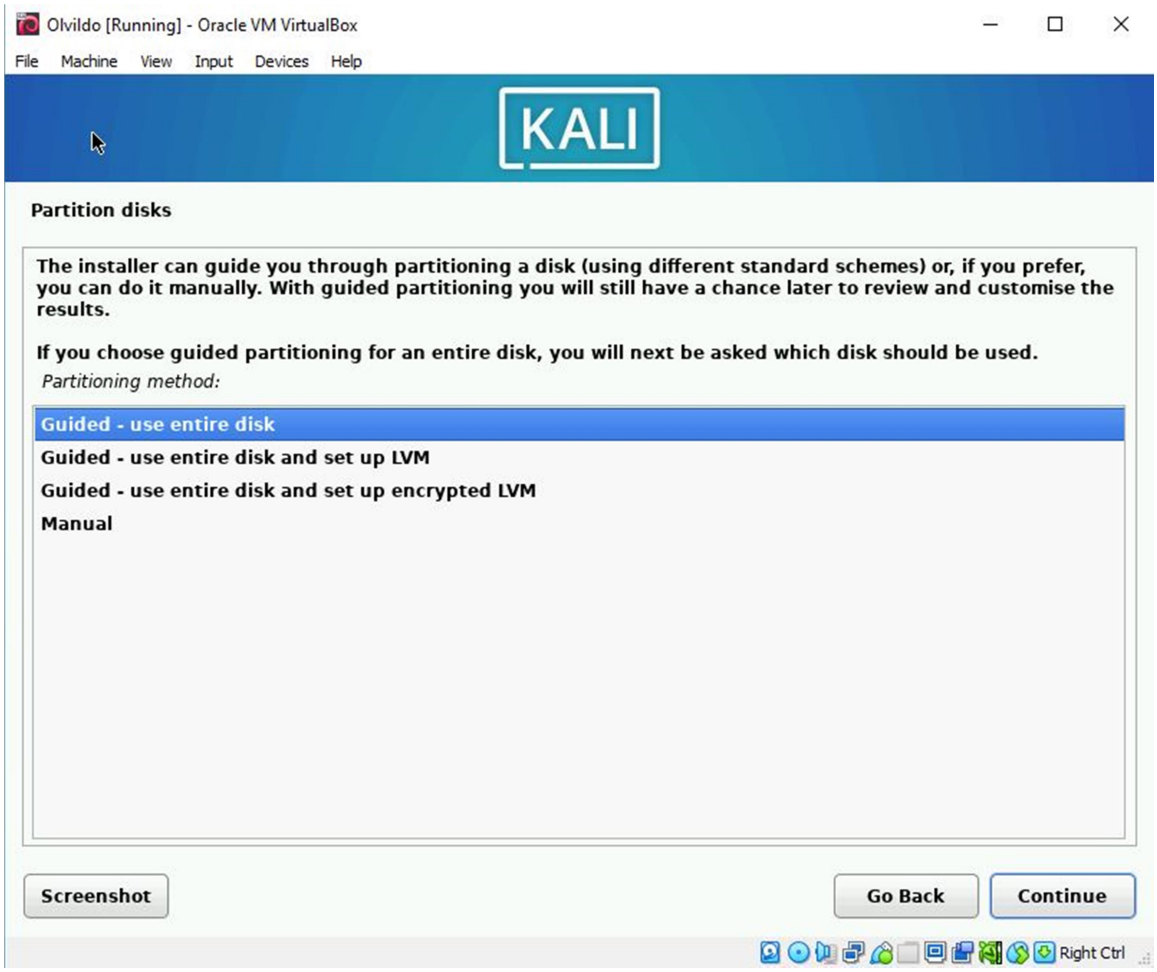

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
Olvildo
Screenshot
Go Back
Continue
Right Ctrl

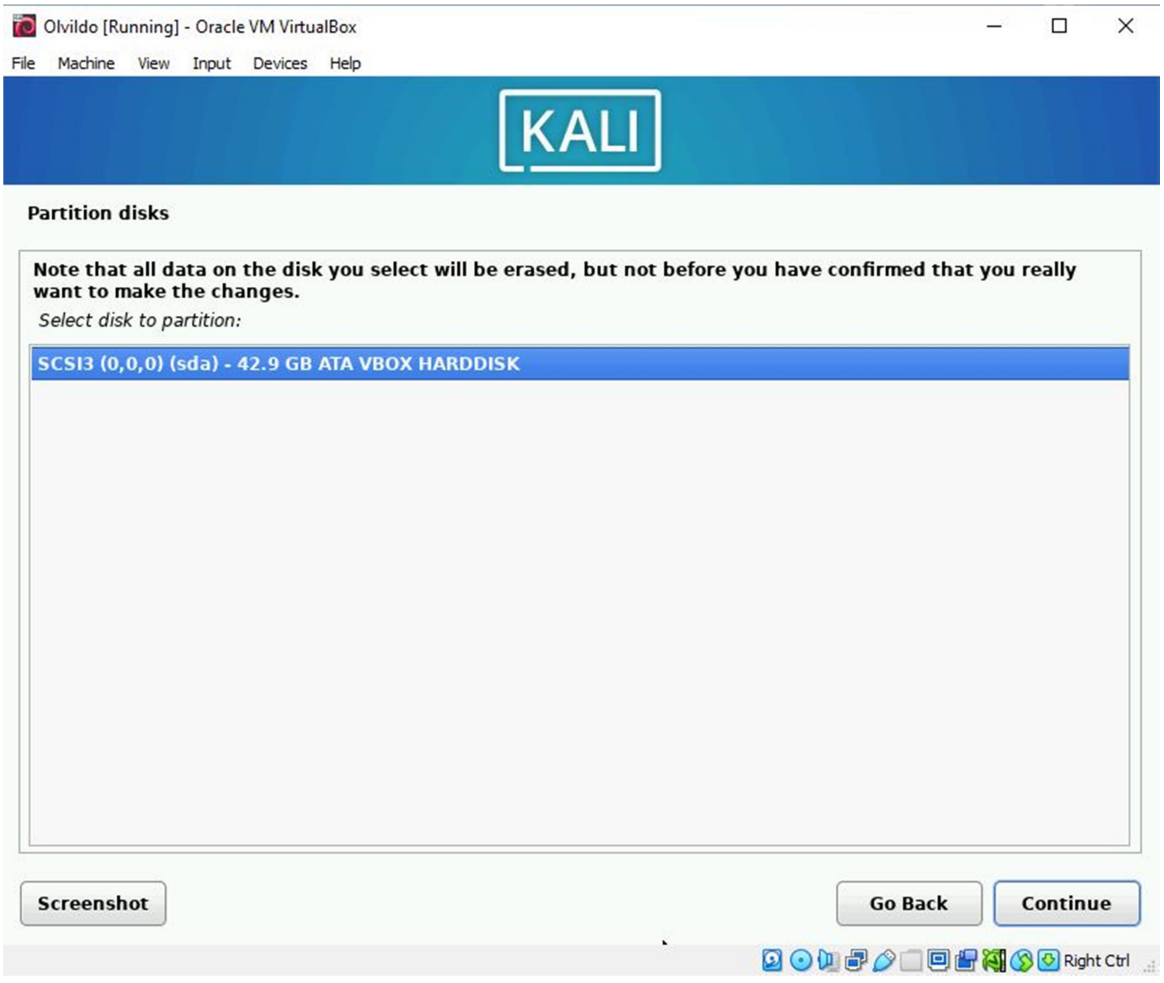

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Configure the network
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.
Domain name:
olvildo
Screenshot
Go Back
Continue
Right Ctrl

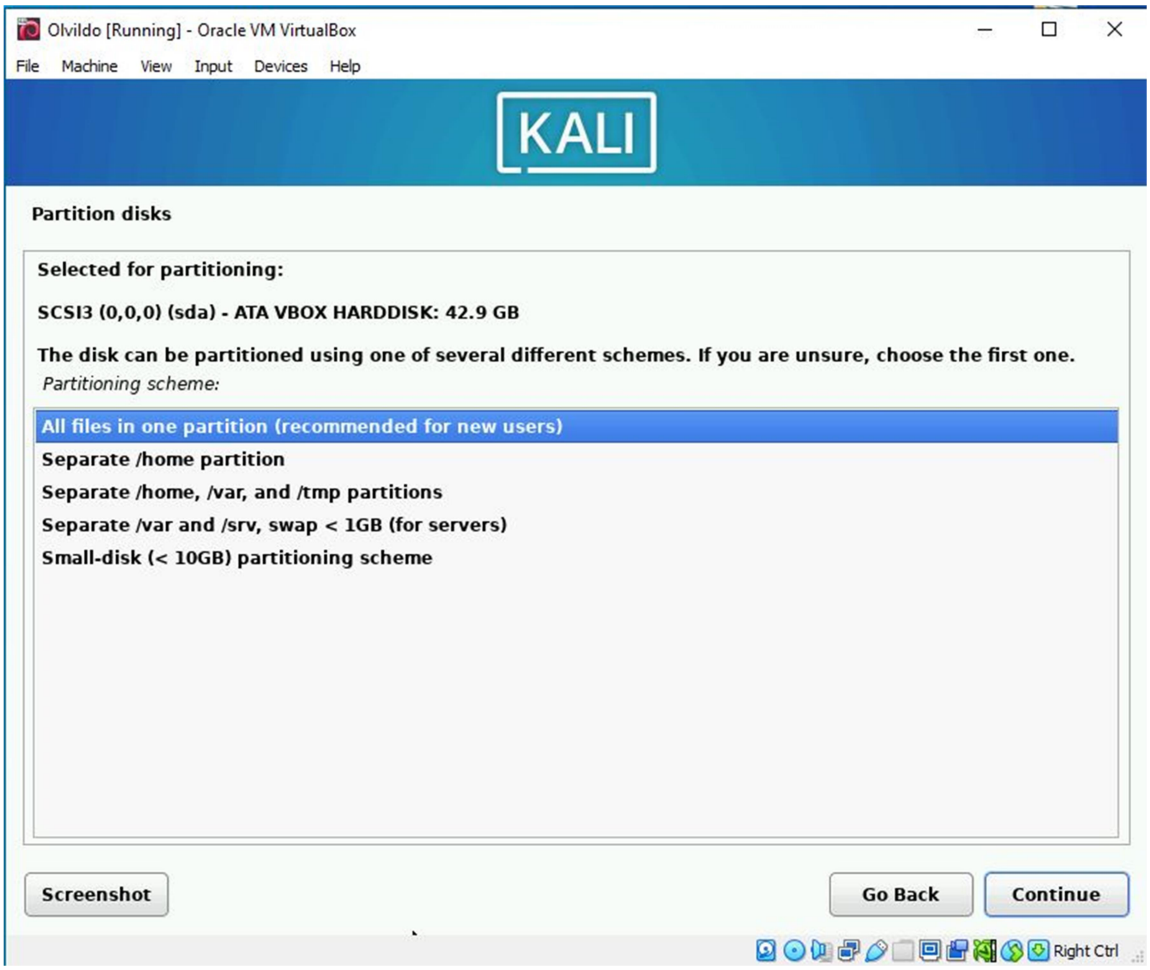

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Set up users and passwords
A user account will be created for you to use instead of the root account for non-administrative activities.
Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.
Full name for the new user:
Saint Louis Valmy
Screenshot
Go Back
Continue
Right Ctrl

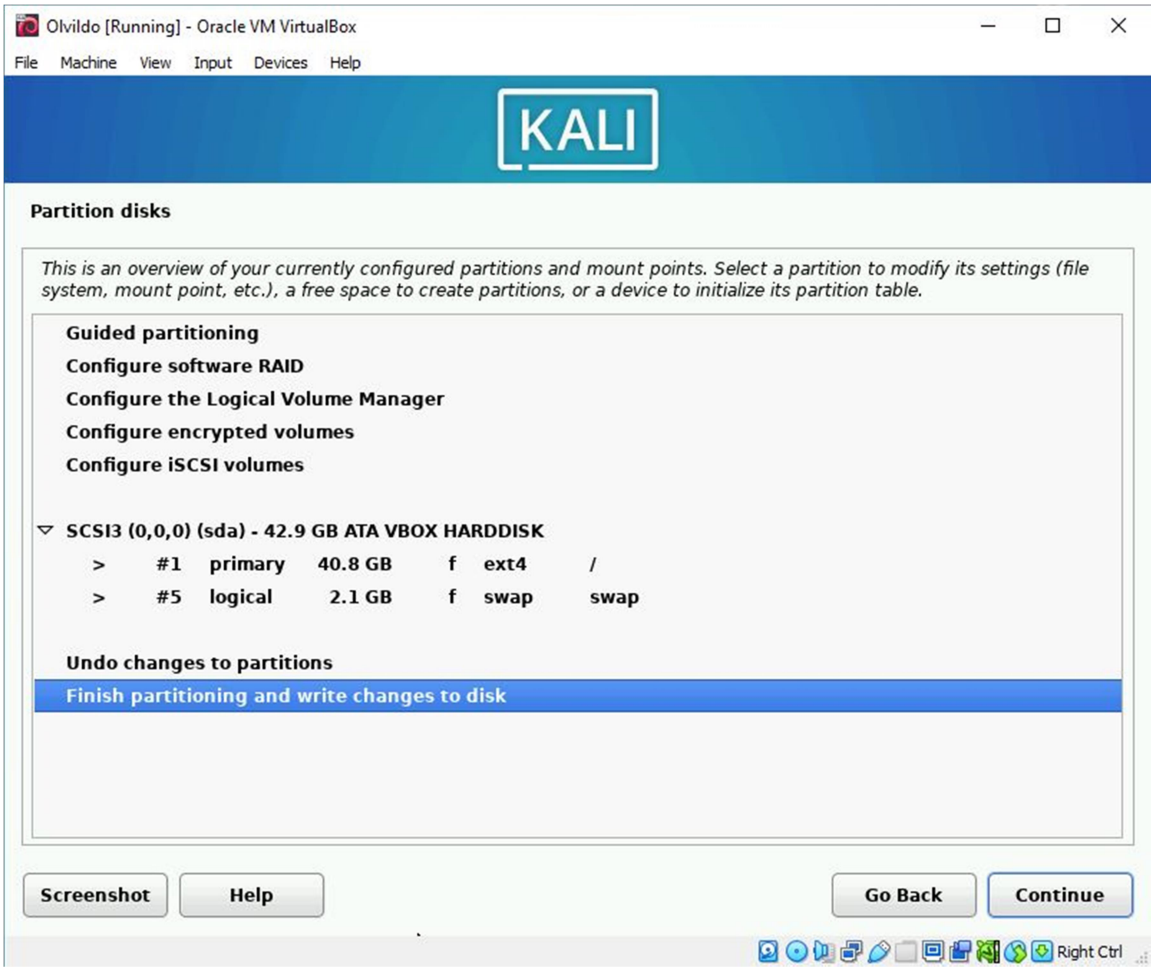

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Set up users and passwords
Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:
olvildo
Screenshot
Go Back
Continue
Right Ctrl

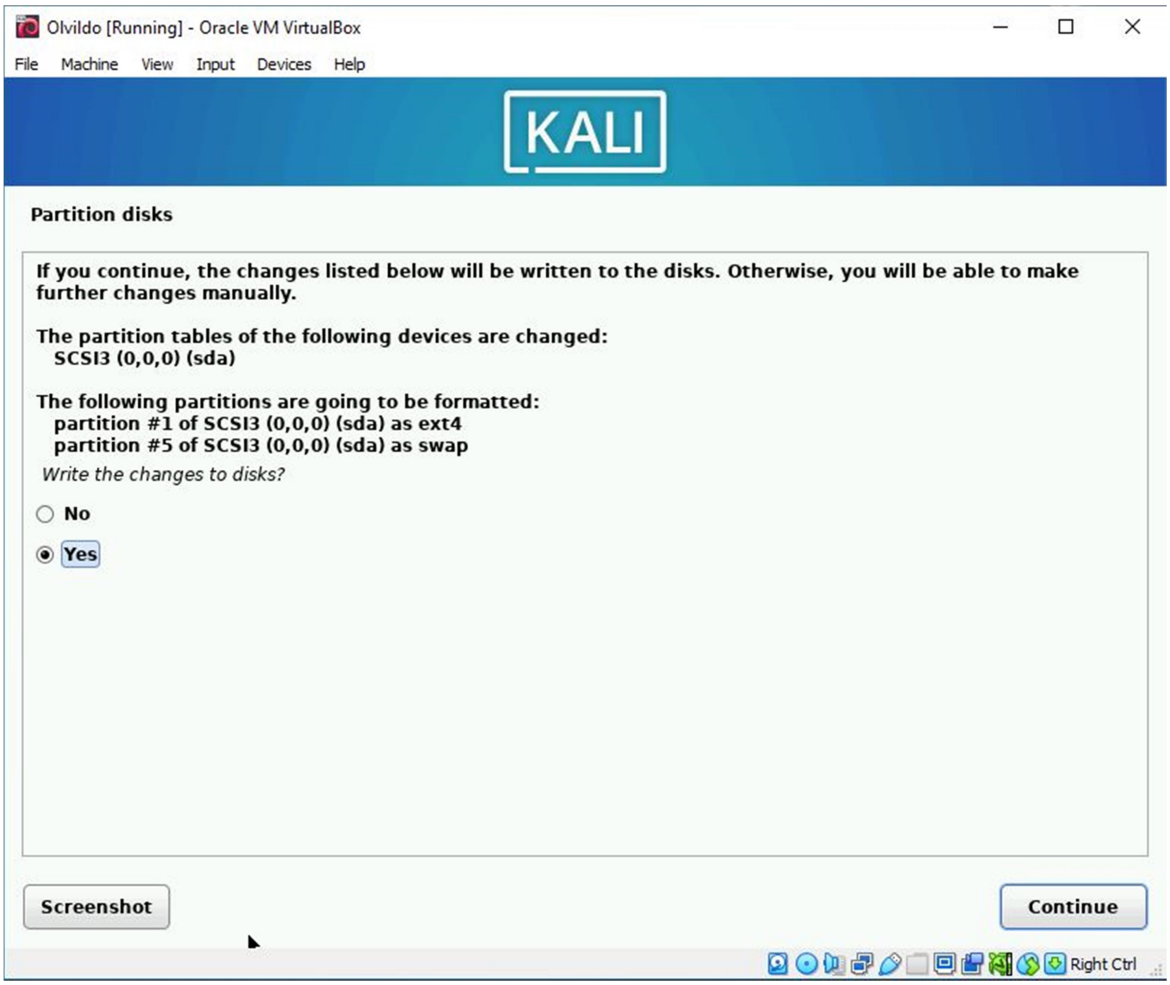

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Set up users and passwords
Make sure to select a strong password that cannot be guessed.
Choose a password for the new user:
Show Password in Clear
Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:
Show Password in Clear
Screenshot
Go Back
Continue
Right Ctrl

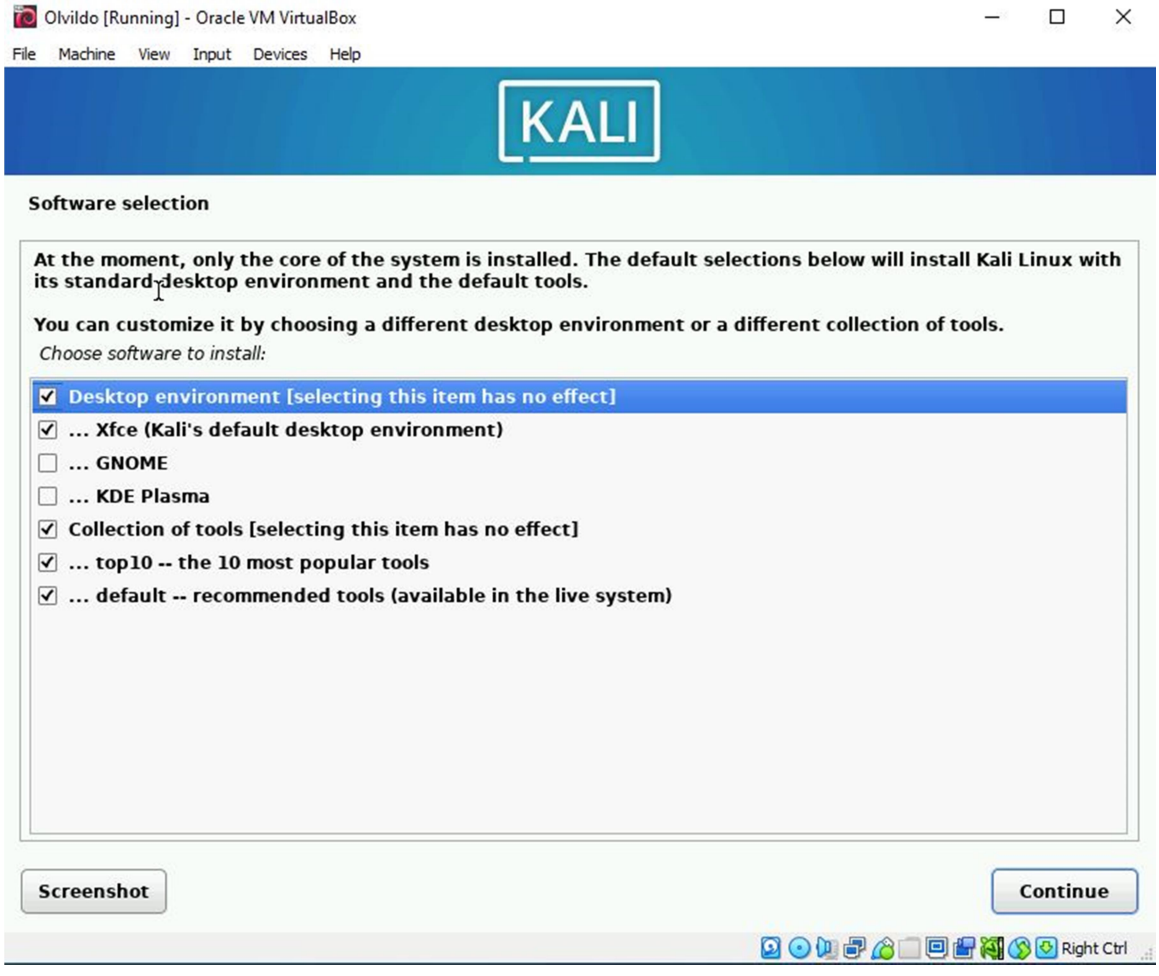

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
Screenshot
Go Back
Continue
Right Ctrl


Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI3 (0,0,0) (sda) - 42.9 GB ATA VBOX HARDDISK
Screenshot
Go Back
Continue
Right Ctrl

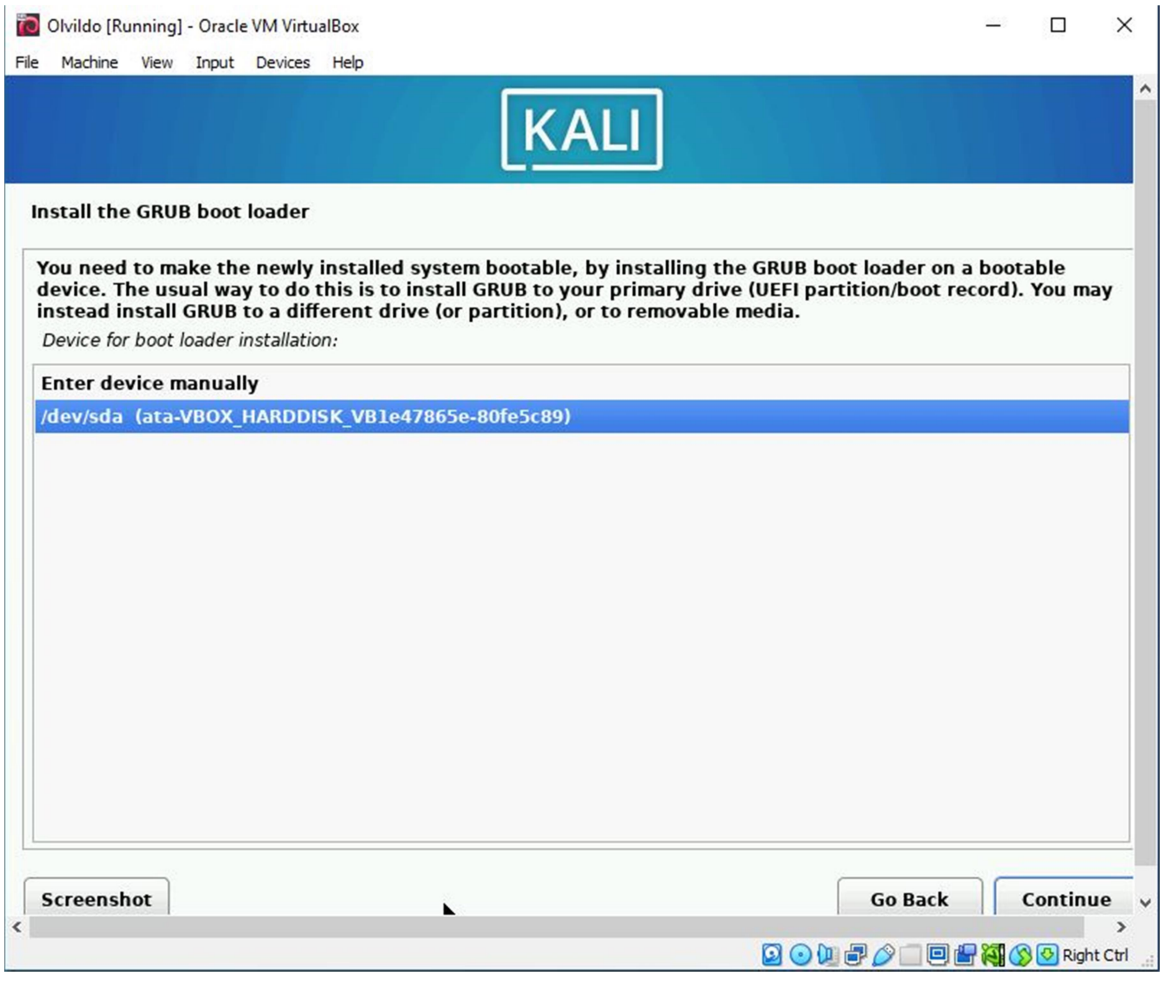

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Partition disks
Selected for partitioning:
SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 42.9 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
Separate /var and /srv, swap < 1GB (for servers)
Small-disk (< 10GB) partitioning scheme
Screenshot
Go Back
Continue
Right Ctrl

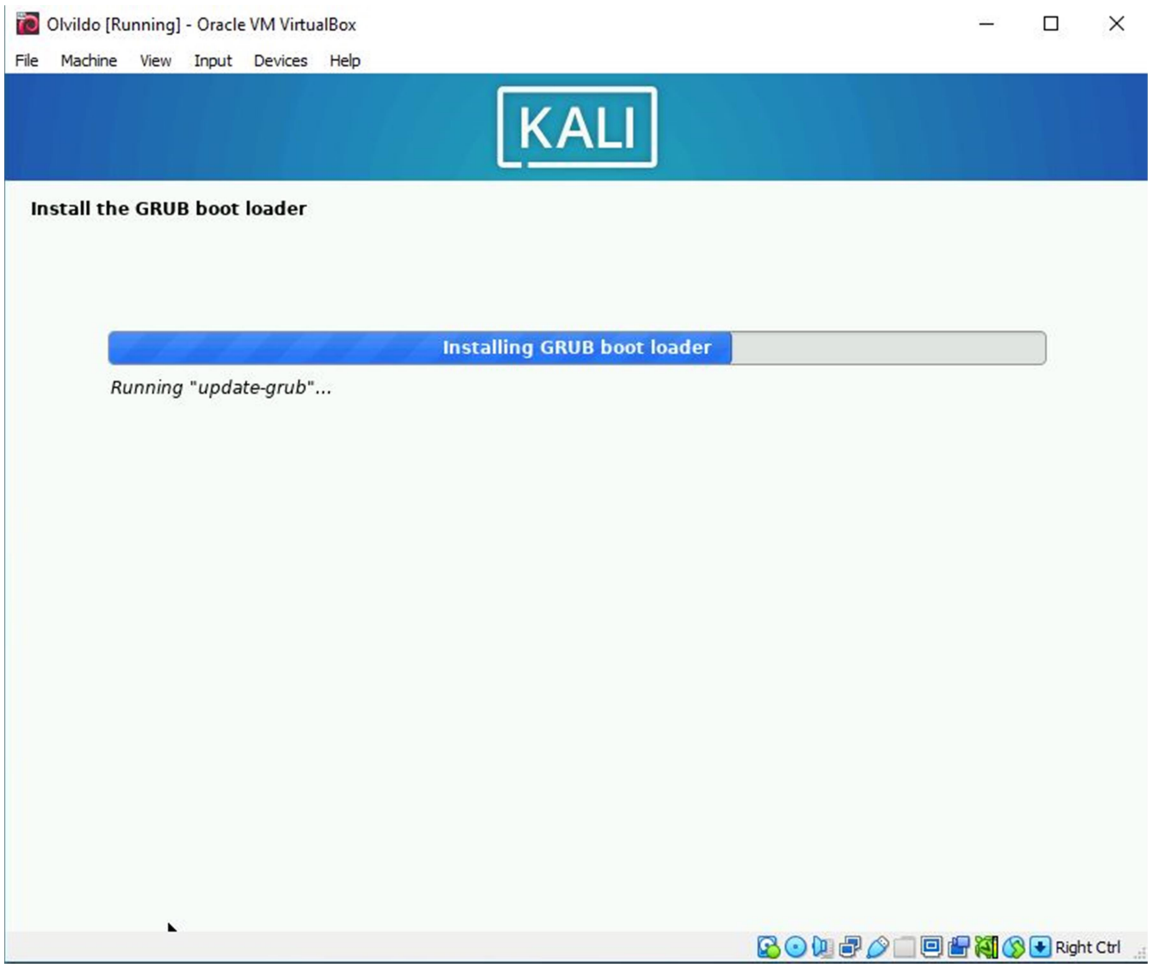

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI3 (0,0,0) (sda) - 42.9 GB ATA VBOX HARDDISK
> #1 primary 40.8 GB f ext4 /
> #5 logical 2.1 GB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
Screenshot
Help
Go Back
Continue
Right Ctrl

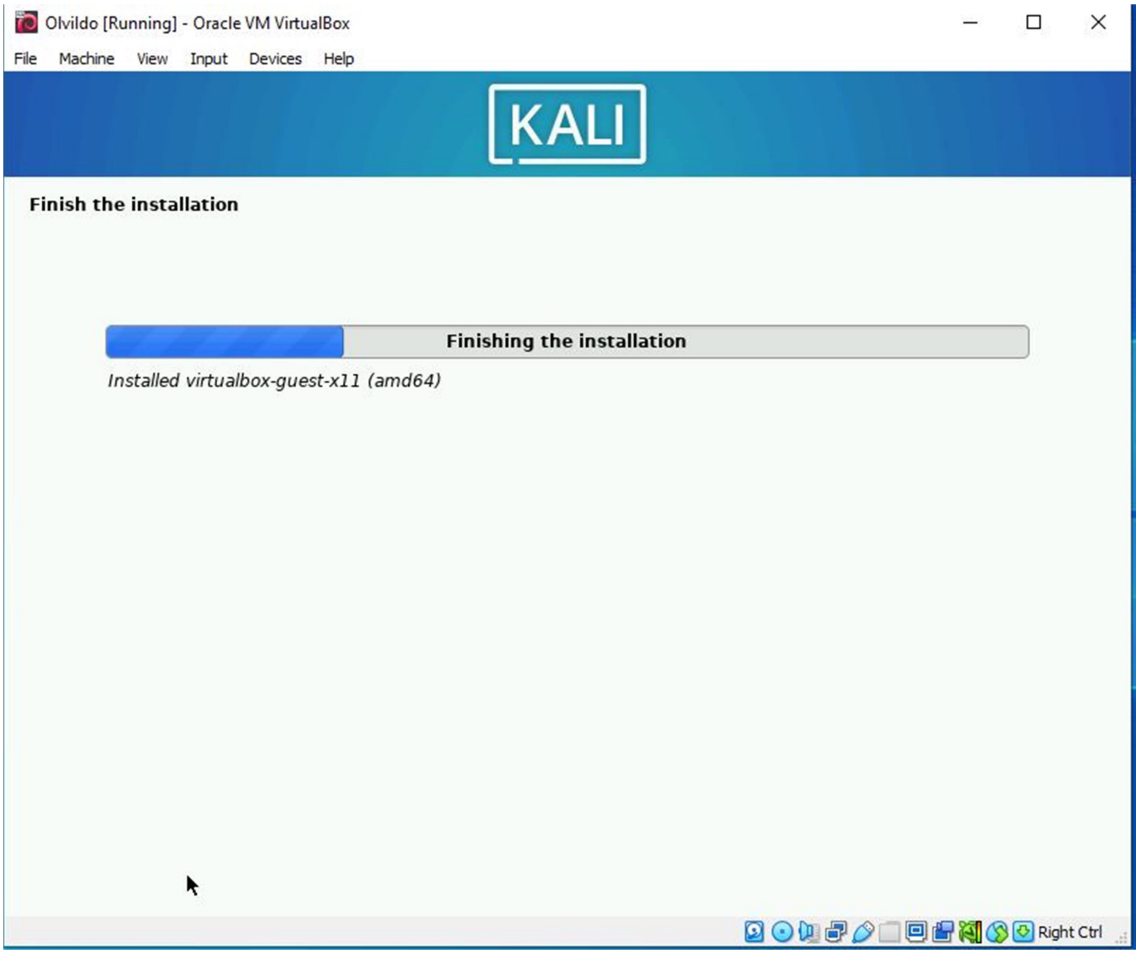

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap
Write the changes to disks?
No
Yes
Screenshot
Continue
Right Ctrl

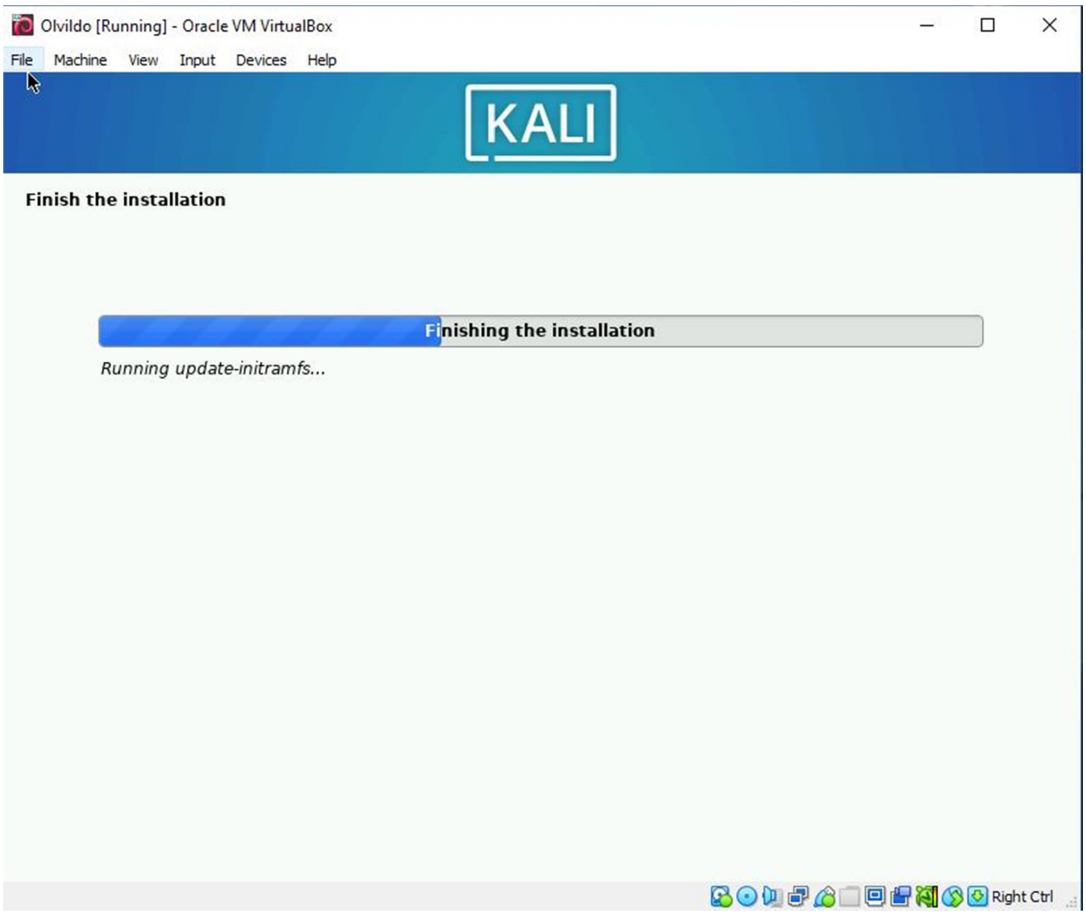

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Software selection
At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.
You can customize it by choosing a different desktop environment or a different collection of tools.
Choose software to install:
Desktop environment [selecting this item has no effect]
... Xfce (Kali's default desktop environment)
... GNOME
... KDE Plasma
Collection of tools [selecting this item has no effect]
... top10 -- the 10 most popular tools
... default -- recommended tools (available in the live system)
Screenshot
Continue
Right Ctrl

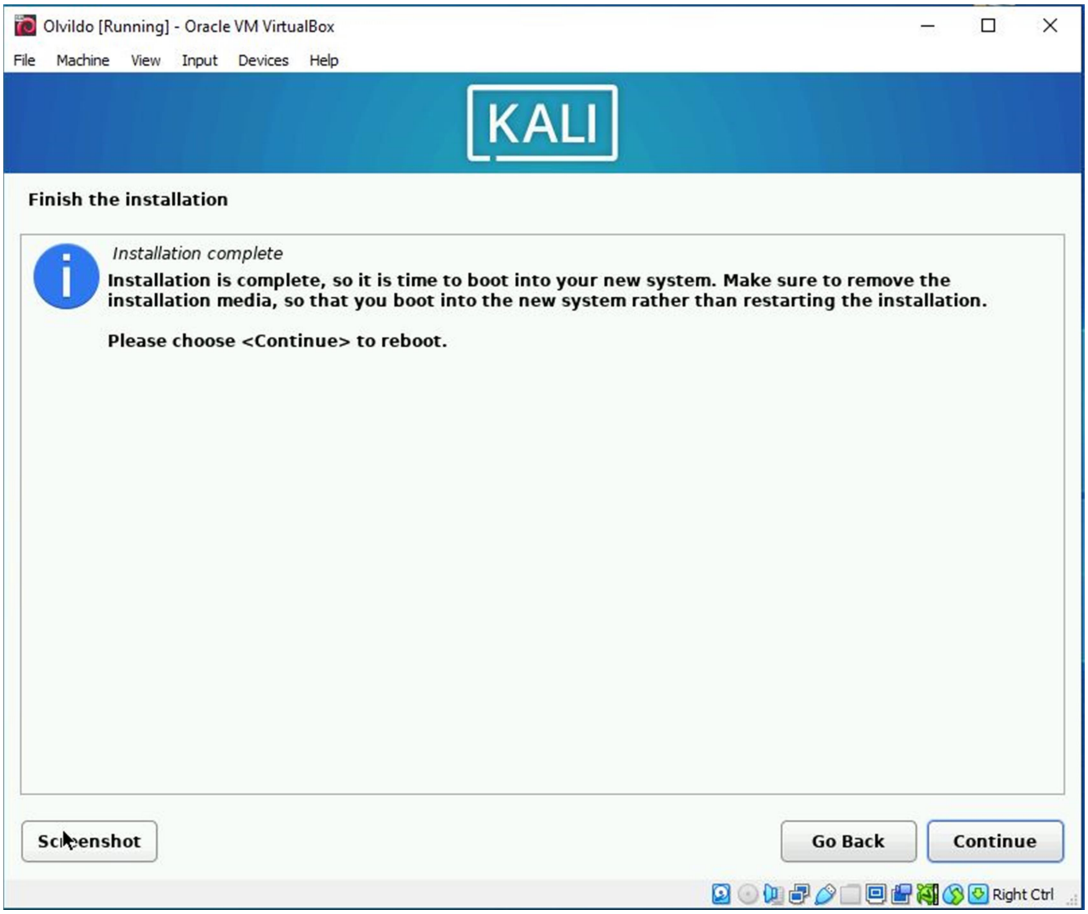

Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Install the GRUB boot loader
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to your primary drive?
No
Yes
Screenshot
Go Back
Continue
Right Ctrl


Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Install the GRUB boot loader
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.
Device for boot loader installation:
Enter device manually
/dev/sda (ata-VBOX_HARDDISK_VB1e47865e-80fe5c89)
Screenshot
Go Back
Continue
Right Ctrl


Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Install the GRUB boot loader
Installing GRUB boot loader
Running "update-grub"...
Right Ctrl


Olvildo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Finish the installation
Finishing the installation
Installed virtualbox-guest-x11 (amd64)
Right Ctrl

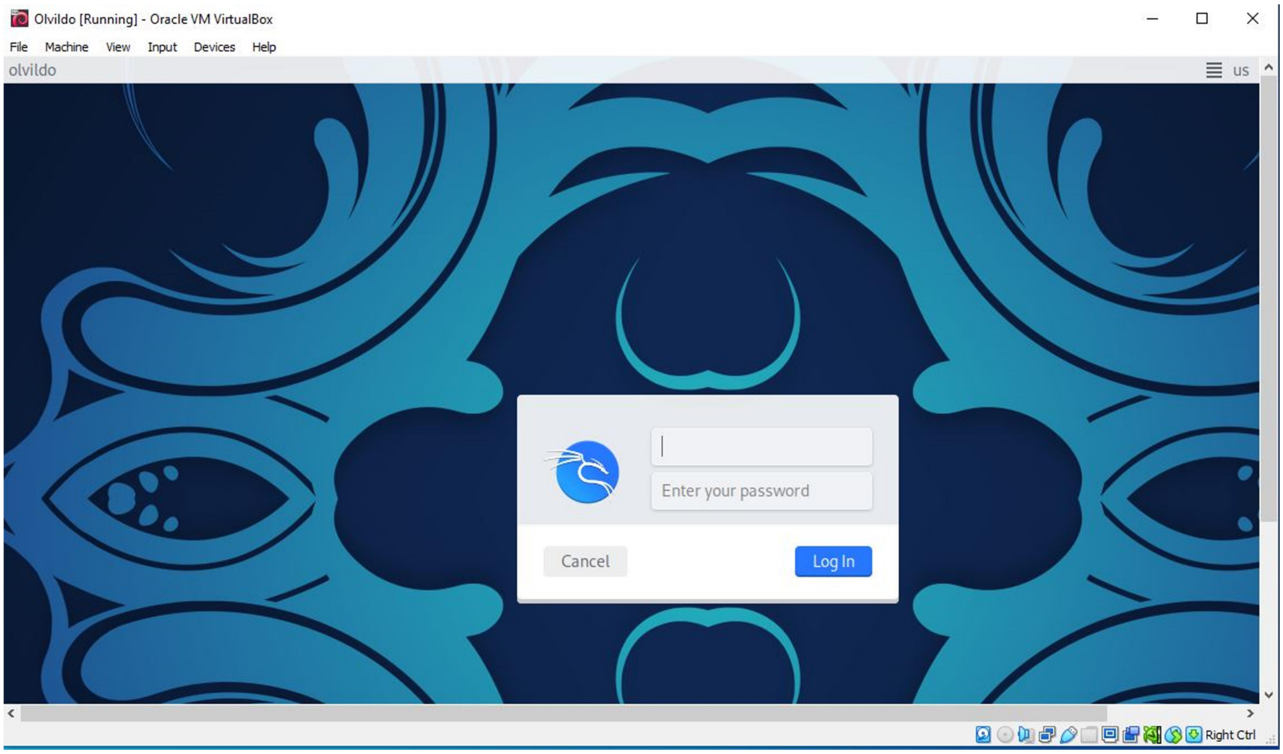




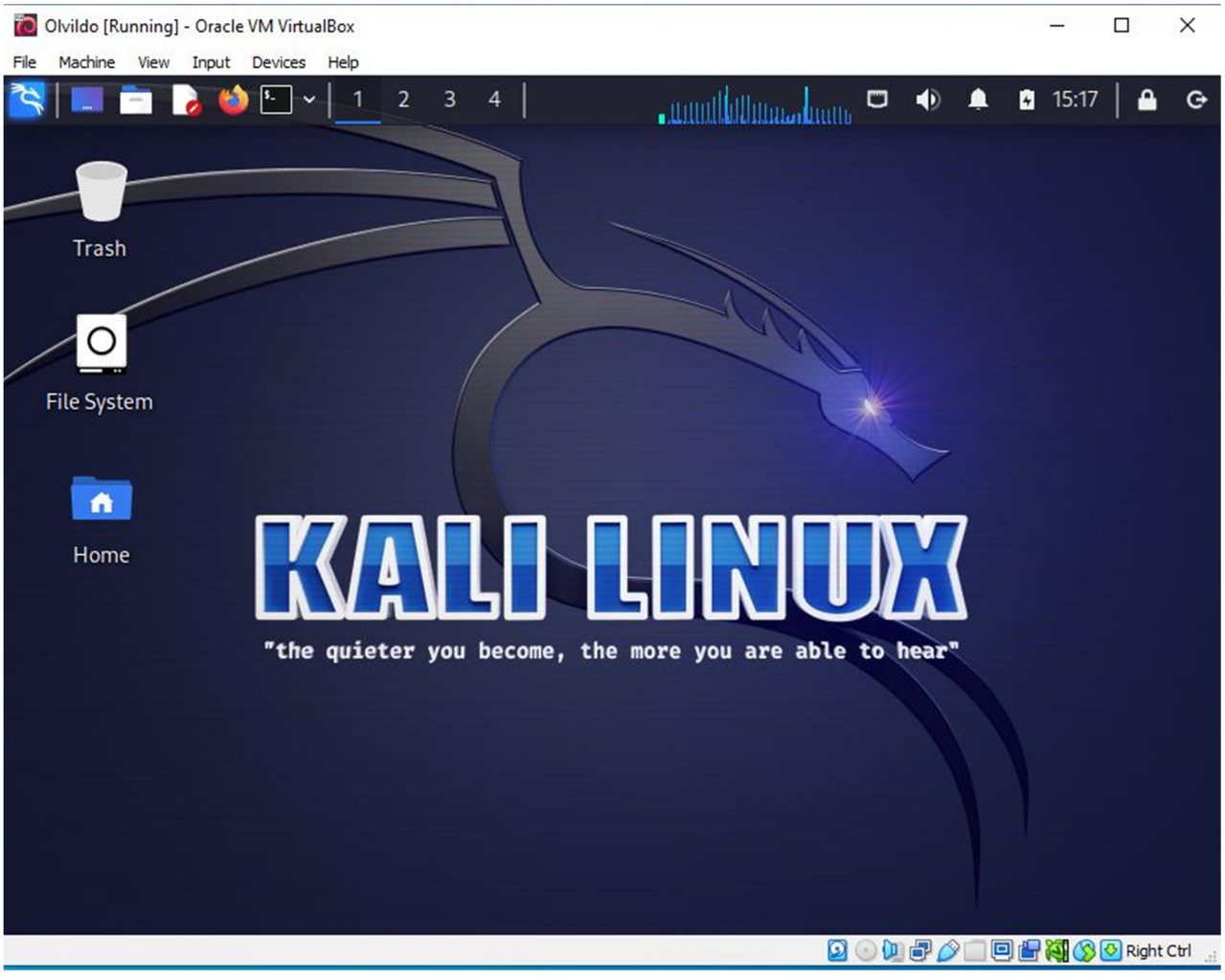
L’installation de système d’exploitation Kali Linux est terminée.

Lancement du système d’exploitation Kali Linux

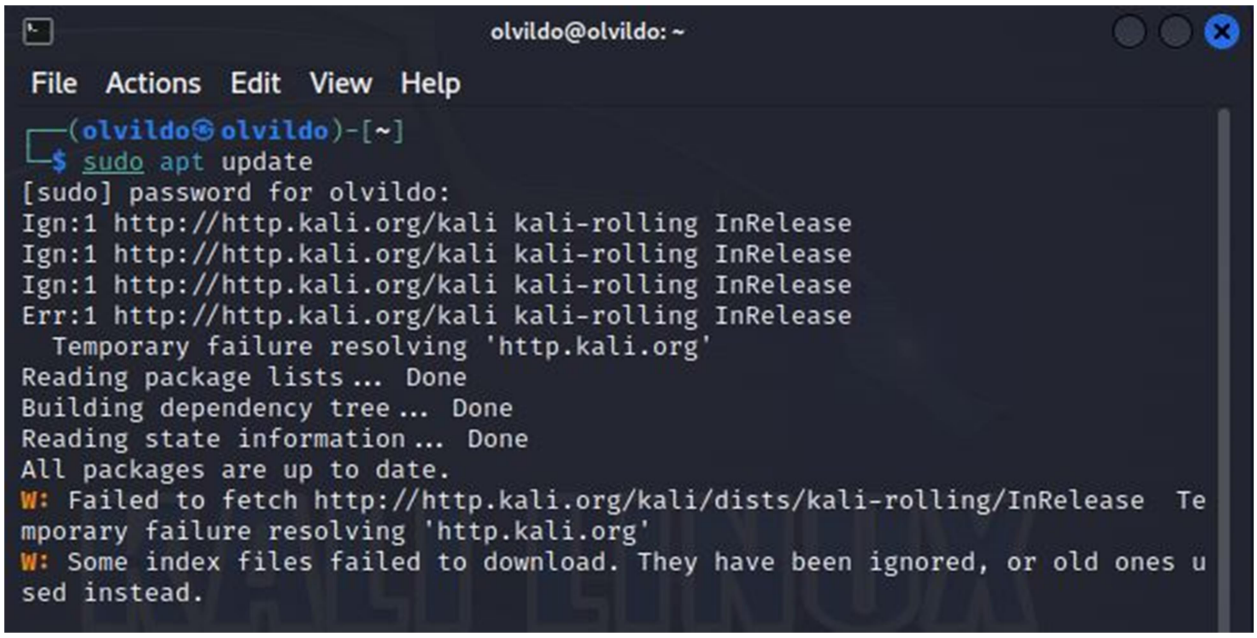
Log in

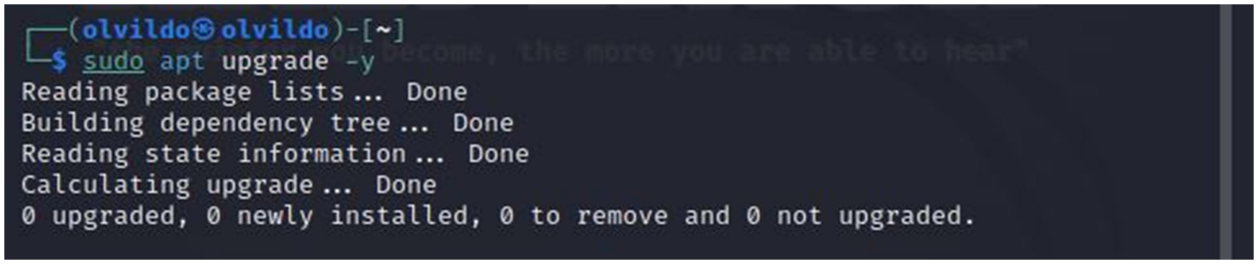


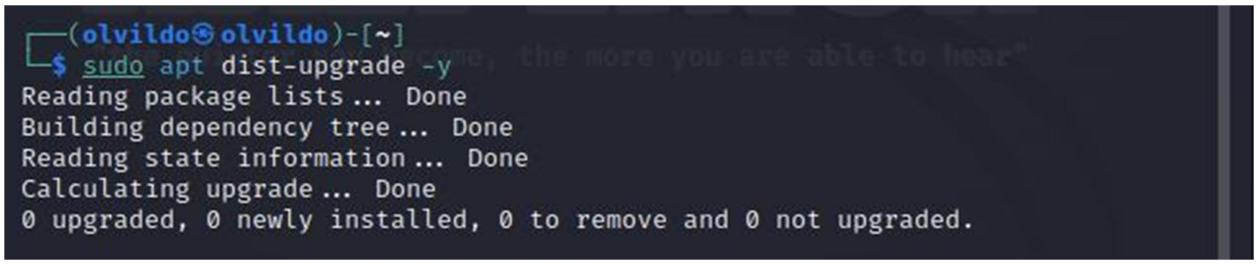
Interface du bureau du système d’exploitation Kali Linux



3. Mise à jour du système après l'installation

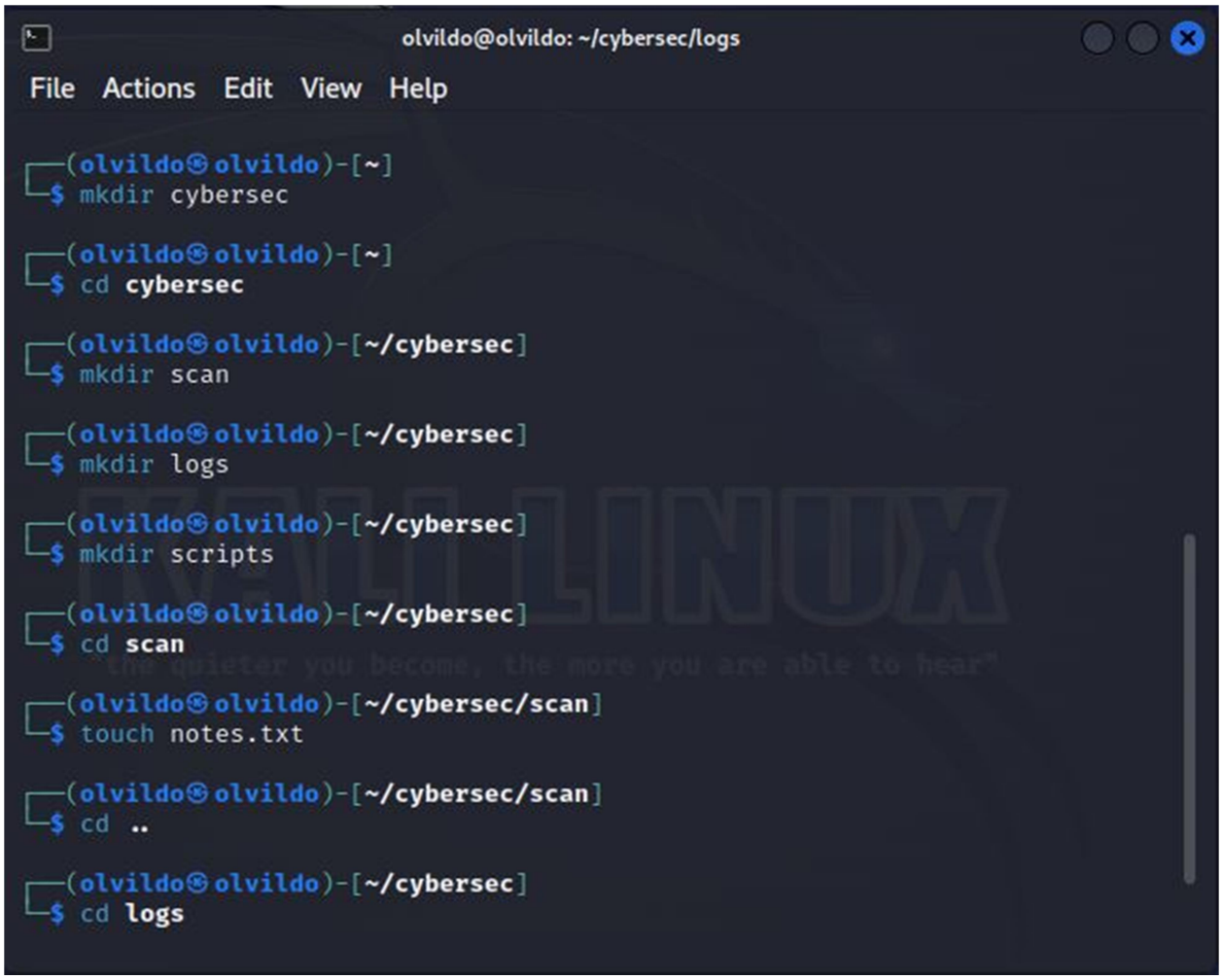






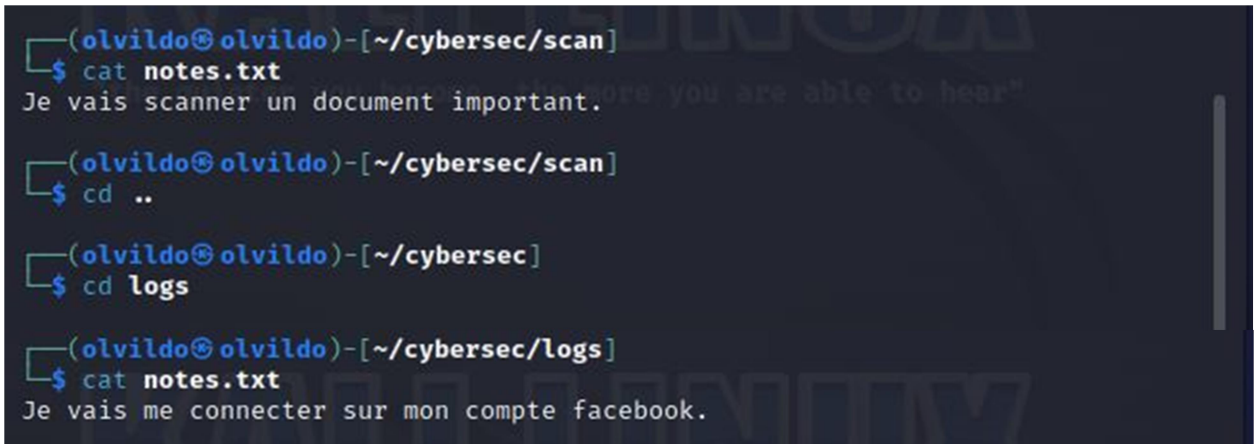
4. Création d'une structure de dossier

- Création du dossier **cybersec** avec trois sous dossiers : **scan, logs, scripts.**

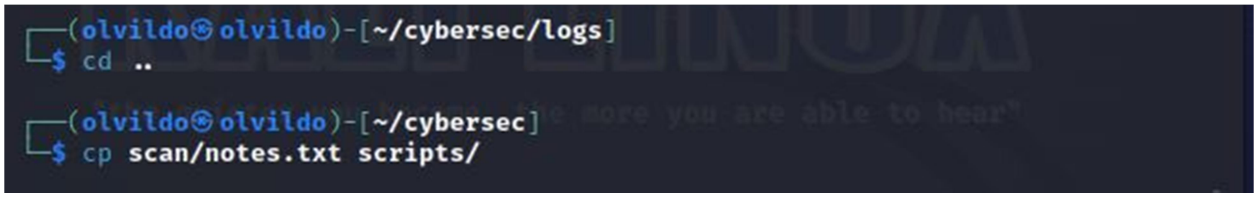


- Ajout du fichier **notes.txt** dans **scan** et **logs**.
- Ajout du contenu dans les fichiers textes (**notes.txt**)

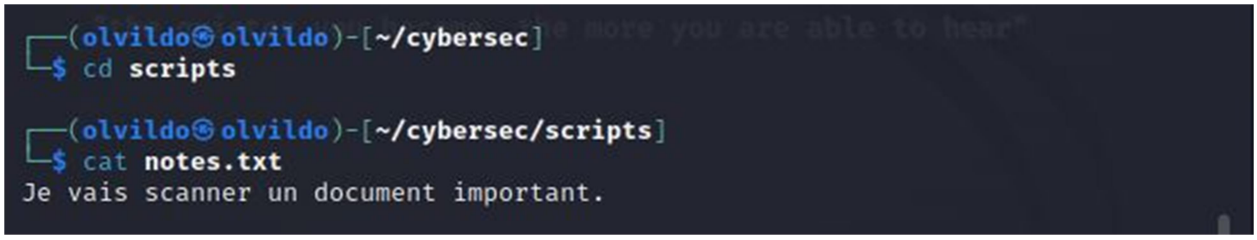
- Affichage du contenu des fichiers.



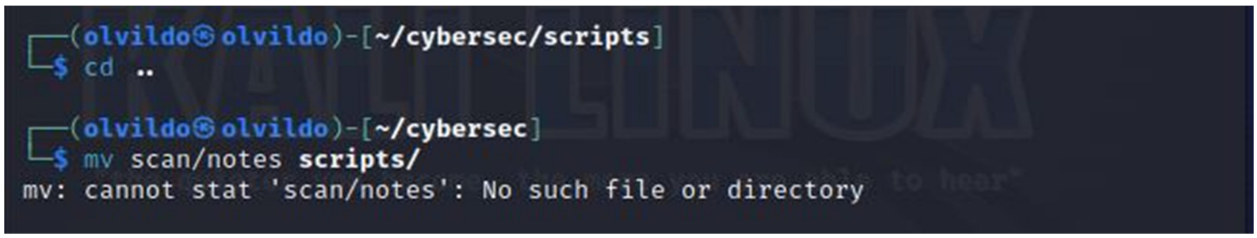
- Copie du fichier (**notes.txt**) dans le sous dossier **scripts.**



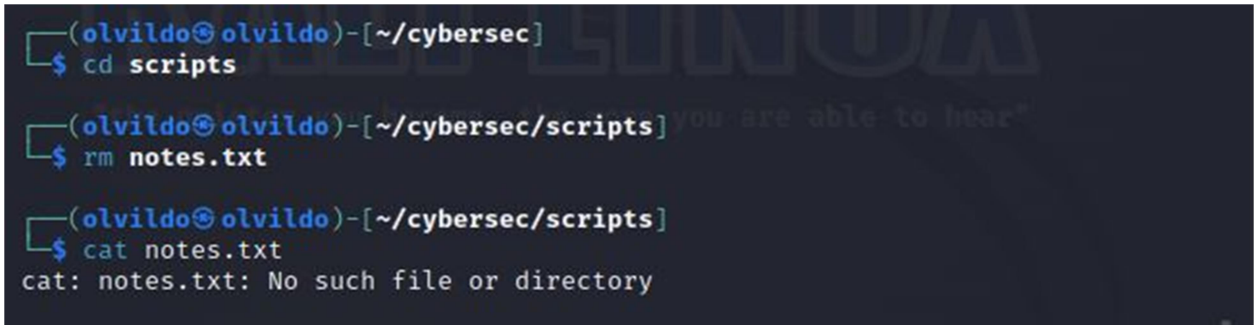
- Vérification de la copie du fichier.



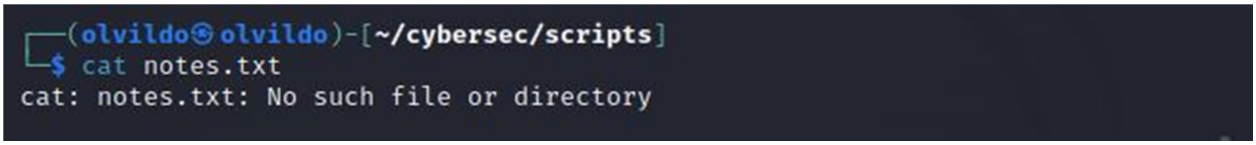
- Déplacement du fichier (**notes.txt**) dans le sous dossier **scan.**



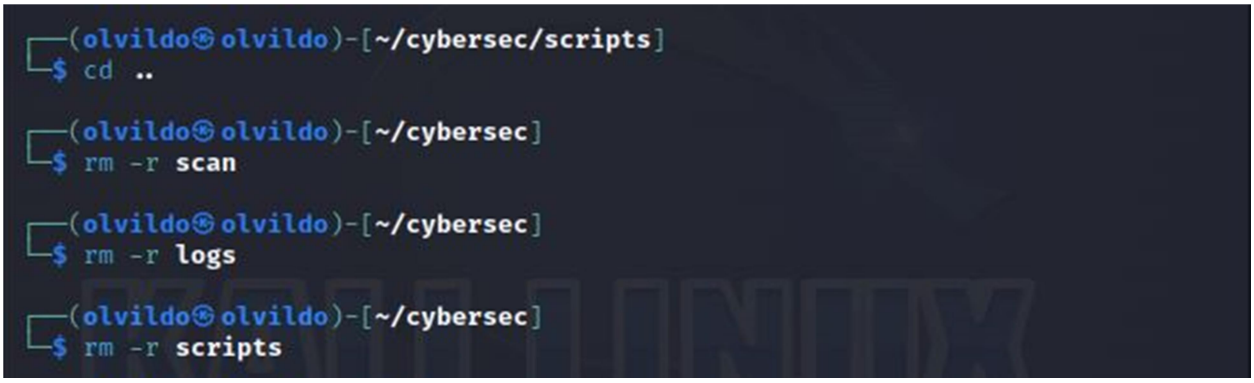
- Suppression du fichier (**notes.txt**) dans le sous dossier **scripts.**



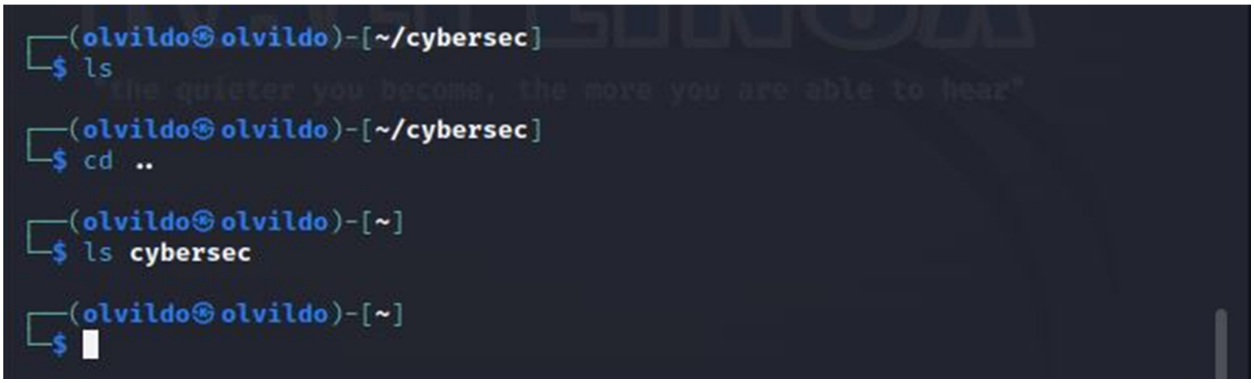
- Vérification de la suppression de fichier.



- Suppression des sous dossiers : **scan**, **logs**, **scripts**

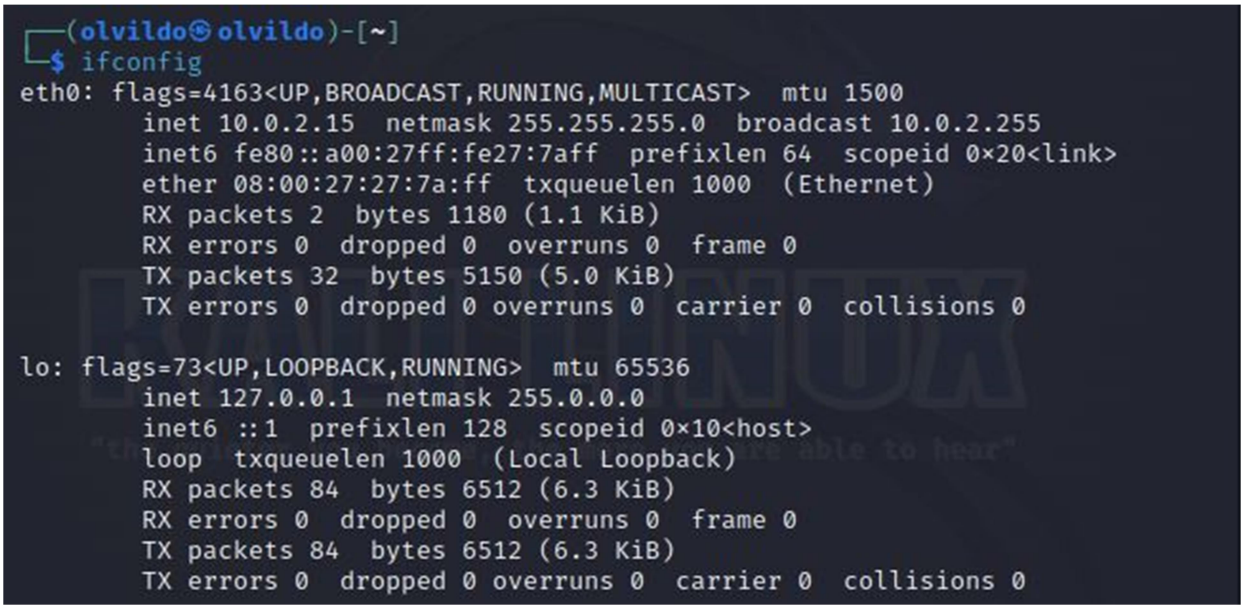


- Vérification de la suppression des sous-dossiers.

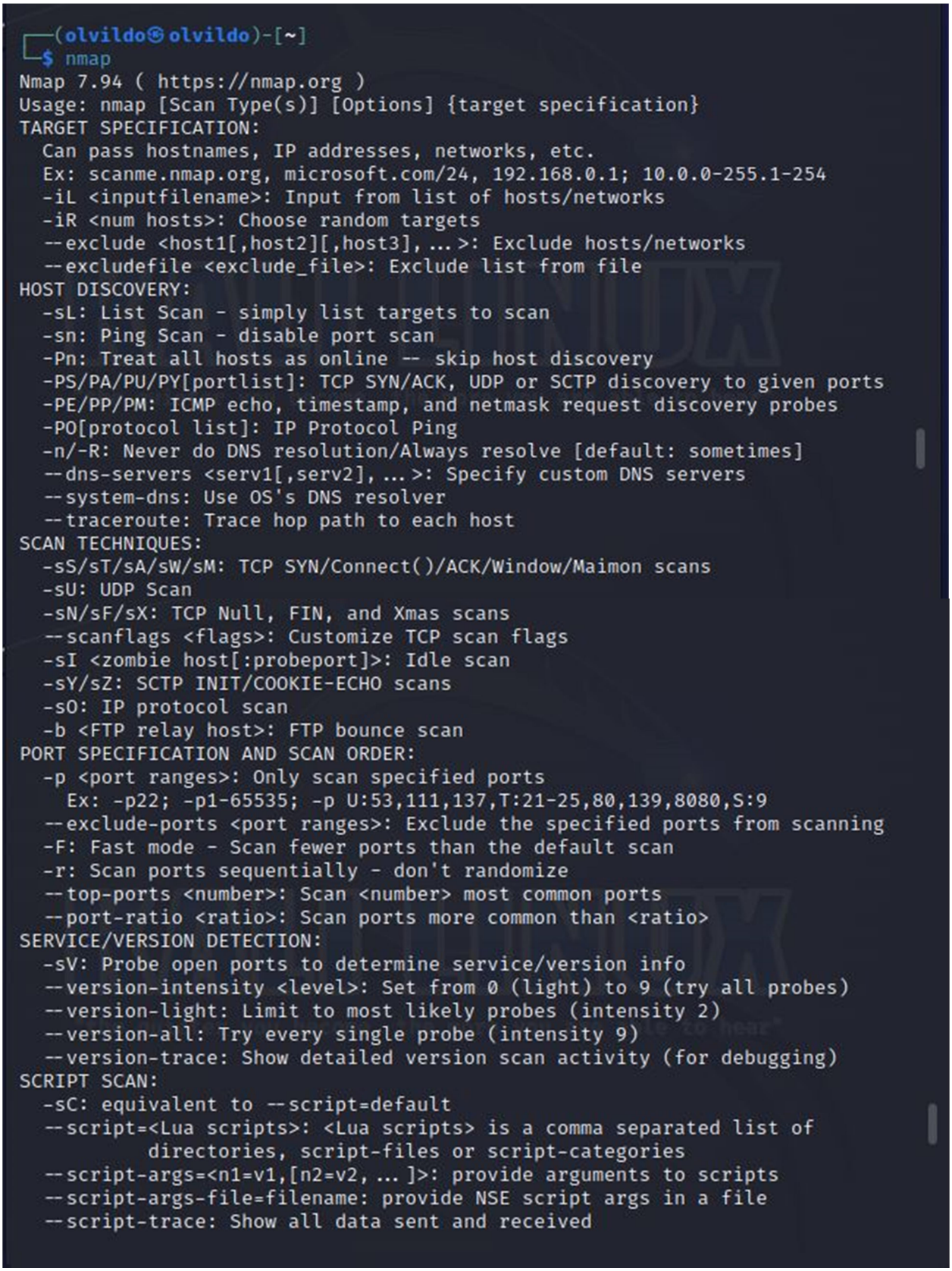


5. Scanner un réseau

- Affichage des informations réseaux



- Utilisation de **nmap** pour scanner un réseau local et identifier les appareils connectés.



```
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
```

```
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPL
ES
```

6. Manipulation des permissions

- Création d'un fichier secret.txt et changement de ses permissions pour qu'il ne soit accessible qu'en lecture par le propriétaire.

```
┌──(olvildo㉿olvildo)-[~]
└─$ touch secret.txt

┌──(olvildo㉿olvildo)-[~]
└─$ chmod 400 secret.txt
```

7. **Utilisation de « grep »**

- Création d'un fichier log.txt avec des lignes de texte, puis utilisation de grep pour rechercher un mot spécifique

```
┌──(olvildo㉿olvildo)-[~]
└─$ touch log.txt

┌──(olvildo㉿olvildo)-[~]
└─$ nano log.txt

┌──(olvildo㉿olvildo)-[~]
└─$ grep "paysan" log.txt
c'est le travailleur, patre, ouvrier, paysan
```

8. Exécution de commandes

```
┌──(olvildo㉿olvildo)-[~]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            945M     0  945M   0% /dev
tmpfs           197M  984K  196M   1% /run
/dev/sda1        39G   13G   24G  36% /
tmpfs           984M     0  984M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           197M  120K  197M   1% /run/user/1000
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ du -sh
1.9M    .
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ free -h
               total        used        free      shared  buff/cache   availa
ble
Mem:           1.9Gi       692Mi       914Mi       7.5Mi       515Mi       1.
2Gi
Swap:          974Mi          0B       974Mi
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.6  20880 12624 ?        Ss   15:12   0:04 /sbin/init
root           2  0.0  0.0      0     0 ?        S    15:12   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   15:12   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   15:12   0:00 [rcu_par_g
root           5  0.0  0.0      0     0 ?        I<   15:12   0:00 [slub_flus
root           6  0.0  0.0      0     0 ?        I<   15:12   0:00 [netns]
root          10  0.0  0.0      0     0 ?        I<   15:12   0:00 [mm_percpu
root          11  0.0  0.0      0     0 ?        I    15:12   0:00 [rcu_tasks
root          12  0.0  0.0      0     0 ?        I    15:12   0:00 [rcu_tasks
root          13  0.0  0.0      0     0 ?        I    15:12   0:00 [rcu_tasks
root          14  0.0  0.0      0     0 ?        S    15:12   0:05 [ksoftirqd
root          15  0.1  0.0      0     0 ?        I    15:12   0:09 [rcu_preem
root          16  0.0  0.0      0     0 ?        S    15:12   0:00 [migration
root          17  0.0  0.0      0     0 ?        S    15:12   0:00 [idle_inje
root          19  0.0  0.0      0     0 ?        S    15:12   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    15:12   0:00 [kdevtmpfs
root          22  0.0  0.0      0     0 ?        I<   15:12   0:00 [inet_frag
root          23  0.0  0.0      0     0 ?        S    15:12   0:00 [kauditd]
root          24  0.0  0.0      0     0 ?        S    15:12   0:00 [khungtask
root          26  0.0  0.0      0     0 ?        S    15:12   0:00 [oom_reape
root          27  0.0  0.0      0     0 ?        I<   15:12   0:00 [writeback
root          29  0.0  0.0      0     0 ?        S    15:12   0:01 [kcompactd
root          30  0.0  0.0      0     0 ?        SN   15:12   0:00 [ksmd]
root          31  0.0  0.0      0     0 ?        SN   15:12   0:00 [khugepage
```

```
root          32  0.0  0.0      0     0 ?        I<   15:12   0:00 [kintegrit
root          33  0.0  0.0      0     0 ?        I<   15:12   0:00 [kblockd]
root          34  0.0  0.0      0     0 ?        I<   15:12   0:00 [blkcg_pun
root          35  0.0  0.0      0     0 ?        I<   15:12   0:00 [tpm_dev_w
root          36  0.0  0.0      0     0 ?        I<   15:12   0:00 [edac-poll
root          37  0.0  0.0      0     0 ?        I<   15:12   0:00 [devfreq_w
root          38  0.0  0.0      0     0 ?        I<   15:12   0:00 [kworker/0
root          39  0.0  0.0      0     0 ?        S    15:12   0:00 [kswapd0]
root          46  0.0  0.0      0     0 ?        I<   15:12   0:00 [kthrotld]
root          48  0.0  0.0      0     0 ?        I<   15:12   0:00 [acpi_ther
root          49  0.0  0.0      0     0 ?        S    15:12   0:00 [xenbus_pr
root          50  0.0  0.0      0     0 ?        I<   15:12   0:00 [mld]
root          51  0.0  0.0      0     0 ?        I<   15:12   0:00 [ipv6_addr
root          56  0.0  0.0      0     0 ?        I<   15:12   0:00 [kstrp]
root          61  0.0  0.0      0     0 ?        I<   15:12   0:00 [zswap-shr
root          62  0.0  0.0      0     0 ?        I<   15:12   0:00 [kworker/u
root         130  0.0  0.0      0     0 ?        I<   15:12   0:00 [cryptd]
root         133  0.0  0.0      0     0 ?        I<   15:12   0:00 [ata_sff]
root         134  0.0  0.0      0     0 ?        S    15:12   0:00 [scsi_eh_0
root         136  0.0  0.0      0     0 ?        I<   15:12   0:00 [scsi_tmf_
root         137  0.0  0.0      0     0 ?        S    15:12   0:00 [scsi_eh_1
root         138  0.0  0.0      0     0 ?        I<   15:12   0:00 [scsi_tmf_
root         141  0.0  0.0      0     0 ?        S    15:12   0:00 [scsi_eh_2
root         142  0.0  0.0      0     0 ?        I<   15:12   0:00 [scsi_tmf_
root         157  0.0  0.0      0     0 ?        S    15:12   0:00 [irq/18-vm
root         158  0.0  0.0      0     0 ?        I<   15:12   0:00 [ttm]
root         159  0.0  0.0      0     0 ?        I<   15:12   0:05 [kworker/0
root         212  0.0  0.0      0     0 ?        S    15:12   0:00 [jbd2/sda1
root         213  0.0  0.0      0     0 ?        I<   15:12   0:00 [ext4-rsv-
root         269  0.0  1.0  49968 20560 ?        Ss   15:13   0:01 /lib/syste
root         284  0.0  0.0      0     0 ?        S    15:13   0:00 [psimon]
root         315  0.0  0.3  27896  7780 ?        Ss   15:13   0:03 /lib/syste
root         342  0.0  0.2   8264  4912 ?        Ss   15:13   0:01 /usr/sbin/
root         354  0.0  0.0      0     0 ?        I<   15:13   0:00 [rpciod]
root         355  0.0  0.0      0     0 ?        I<   15:13   0:00 [xprtiod]
root         369  0.0  0.0      0     0 ?        S    15:13   0:00 [psimon]
root         517  0.0  0.1   7016  2432 ?        Ss   15:13   0:00 /usr/sbin/
message+     518  0.0  0.2  10664  5760 ?        Ss   15:13   0:04 /usr/bin/d
polkitd      520  0.0  0.4 310460  9980 ?        Ssl  15:13   0:02 /usr/lib/p
root         521  0.0  0.4  17484  8704 ?        Ss   15:13   0:00 /lib/syste
root         543  0.0  0.0      0     0 ?        S    15:13   0:00 [psimon]
root         552  0.0  1.0 333308 21544 ?        Ssl  15:13   0:01 /usr/sbin/
root         564  0.0  0.6 317448 12240 ?        Ssl  15:13   0:00 /usr/sbin/
root         575  0.0  0.1 293332  3456 ?        Sl   15:13   0:06 /usr/sbin/
root         599  0.0  0.3 382660  7508 ?        SLsl 15:13   0:00 /usr/sbin/
root         619  2.3  4.8 386236 96700 tty7     Ssl+ 15:13   3:23 /usr/lib/x
root         621  0.0  0.0   5896  1920 tty1     Ss+  15:13   0:00 /sbin/aget
root         711  0.0  0.0      0     0 ?        S    15:13   0:00 [psimon]
rtkit        742  0.0  0.1  22776  3072 ?        SNsl 15:13   0:01 /usr/libex
root         821  0.0  0.4 236376  8420 ?        Sl   15:15   0:00 lightdm --
olvildo      828  0.0  0.5  19724 11392 ?        Ss   15:15   0:00 /lib/syste
olvildo      829  0.0  0.2  21992  5212 ?        S    15:15   0:00 (sd-pam)
root         843  0.0  0.0      0     0 ?        S    15:15   0:00 [psimon]
olvildo      845  0.0  0.6 118656 14080 ?        S<sl 15:15   0:00 /usr/bin/p
```

```
olvildo      845  0.0  0.6 118656 14080 ?        S<sl 15:15   0:00 /usr/bin/p
olvildo      846  0.0  0.2  94740  5504 ?        Ssl  15:15   0:00 /usr/bin/p
olvildo      847  0.0  1.6 559044 34156 ?        S<sl 15:15   0:00 /usr/bin/w
olvildo      848  0.0  0.4 101400  9088 ?        S<sl 15:15   0:00 /usr/bin/p
olvildo      851  0.0  0.5 314572 11860 ?        SLsl 15:15   0:00 /usr/bin/g
olvildo      856  0.0  0.2   9812  5632 ?        Ss   15:15   0:01 /usr/bin/d
olvildo      872  0.0  1.2 341172 26116 ?        Ssl  15:15   0:01 xfce4-sess
olvildo      926  0.0  0.0  19516  1536 ?        S    15:15   0:00 /usr/bin/V
olvildo      927  0.0  0.1 217704  3968 ?        Sl   15:15   0:00 /usr/bin/V
olvildo      941  0.0  0.0  19516  1664 ?        S    15:15   0:00 /usr/bin/V
olvildo      942  0.1  0.1 217804  3328 ?        Sl   15:15   0:14 /usr/bin/V
olvildo      949  0.0  0.0  19516  1536 ?        S    15:15   0:00 /usr/bin/V
olvildo      950  0.7  0.1 218320  3072 ?        Sl   15:15   0:59 /usr/bin/V
olvildo      961  0.0  0.0   7908  1776 ?        Ss   15:15   0:00 /usr/bin/s
olvildo      976  0.0  0.0  19516  1536 ?        S    15:15   0:00 /usr/bin/V
olvildo      977  0.0  0.2 221764  4864 ?        Sl   15:15   0:04 /usr/bin/V
olvildo      982  0.0  0.4 385032  9932 ?        Ssl  15:15   0:00 /usr/libex
olvildo      989  0.0  0.2   9360  4864 ?        S    15:15   0:00 /usr/bin/d
olvildo     1001  0.0  0.3 238296  7808 ?        Sl   15:15   0:01 /usr/libex
olvildo     1013  0.0  0.2  81684  5200 ?        SLs  15:15   0:00 /usr/bin/g
olvildo     1015  0.5  2.2 544168 45960 ?        Sl   15:15   0:43 xfwm4
olvildo     1019  0.0  0.4 312216  9592 ?        Ssl  15:15   0:00 /usr/libex
olvildo     1025  0.0  0.4 457652  8960 ?        Sl   15:15   0:00 /usr/libex
olvildo     1040  0.0  1.5 305544 30496 ?        Sl   15:15   0:03 xfsettings
root        1054  0.0  0.4 308092  8760 ?        Ssl  15:15   0:01 /usr/libex
olvildo     1061  0.0  2.1 475240 43980 ?        Sl   15:15   0:07 xfce4-pane
olvildo     1066  0.0  2.7 560092 55036 ?        Sl   15:15   0:02 Thunar --d
olvildo     1077  0.0  2.9 566180 59220 ?        Sl   15:15   0:07 xfdesktop
olvildo     1081  0.0  2.4 408424 49560 ?        Sl   15:15   0:02 /usr/lib/x
olvildo     1085  0.0  0.9 260336 18632 ?        Sl   15:15   0:00 /usr/lib/p
olvildo     1086  0.0  1.4 416576 29488 ?        Sl   15:15   0:02 /usr/lib/x
olvildo     1087  0.0  0.5 381968 10204 ?        Sl   15:15   0:00 /usr/libex
olvildo     1090  0.0  2.4 633732 48948 ?        Sl   15:15   0:01 nm-applet
olvildo     1104  0.0  0.5 309692 10684 ?        Sl   15:15   0:00 xiccd
olvildo     1105  0.0  2.6 448708 53812 ?        Sl   15:15   0:02 /usr/bin/p
olvildo     1114  0.0  1.2 266456 26152 ?        Sl   15:15   0:01 xfce4-powe
olvildo     1125  0.0  1.5 571244 30404 ?        Sl   15:15   0:00 light-lock
colord      1129  0.0  0.7 316952 14988 ?        Ssl  15:15   0:00 /usr/libex
olvildo     1132  0.0  0.1  14656  3948 ?        Ssl  15:15   0:00 xcape -e S
olvildo     1139  0.0  0.3 230240  7724 ?        Ssl  15:15   0:00 /usr/libex
olvildo     1217  1.1  1.9 431636 38956 ?        Sl   15:15   1:36 /usr/lib/x
olvildo     1218  0.0  1.3 413916 27104 ?        Sl   15:15   0:00 /usr/lib/x
olvildo     1219  0.5  1.3 415896 28016 ?        Sl   15:15   0:49 /usr/lib/x
olvildo     1220  0.0  2.1 552048 43936 ?        Sl   15:15   0:01 /usr/lib/x
olvildo     1221  0.0  2.3 481140 46620 ?        Sl   15:15   0:01 /usr/lib/x
olvildo     1222  0.0  2.2 407984 45388 ?        Sl   15:15   0:02 /usr/lib/x
olvildo     1223  0.0  2.1 407828 43456 ?        Sl   15:15   0:00 /usr/lib/x
olvildo     1321  0.0  0.8 426180 16748 ?        Ssl  15:16   0:00 /usr/libex
root        1333  0.0  0.7 471072 15988 ?        Ssl  15:16   0:00 /usr/libex
olvildo     1370  0.0  0.3  48856  7680 ?        Ss   15:16   0:00 /usr/libex
olvildo     1371  0.0  0.5 308656 10500 ?        Ssl  15:16   0:00 /usr/libex
olvildo     1377  0.0  0.4 307696  8208 ?        Ssl  15:16   0:00 /usr/libex
```

```
olvildo     1411  0.0  0.5 386192 10608 ?        Sl   15:16   0:00 /usr/libex
olvildo     1431  0.0  0.4 234192  8092 ?        Ssl  15:16   0:00 /usr/libex
olvildo     4415  0.2  5.0 445792 102248 ?       Sl   15:22   0:20 /usr/bin/q
olvildo     4450  0.4  0.3  10864  6480 pts/0    Ss   15:22   0:35 /usr/bin/z
root       45349  0.0  0.0      0     0 ?        I    16:46   0:00 [kworker/u
root       54732  0.0  0.0      0     0 ?        I    17:05   0:00 [kworker/u
root       63169  0.1  0.0      0     0 ?        I    17:22   0:01 [kworker/0
root       64426  0.0  0.0      0     0 ?        I    17:25   0:00 [kworker/u
root       65690  0.0  0.0      0     0 ?        I    17:27   0:00 [kworker/0
root       68192  0.1  0.0      0     0 ?        I    17:32   0:00 [kworker/0
olvildo    69555  0.1  0.3 307460  8048 ?        Sl   17:35   0:00 /usr/lib/x
root       69817  0.0  0.0      0     0 ?        I    17:36   0:00 [kworker/u
olvildo    69998  150  0.2  11724  4608 pts/0    R+   17:36   0:00 ps aux
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:02.0 VGA compatible controller: VMware SVGA II Adapter
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Contr
oller (rev 02)
00:04.0 System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Servi
ce
00:05.0 Multimedia audio controller: Intel Corporation 82801AA AC'97 Audio Co
ntroller (rev 01)
00:06.0 USB controller: Apple Inc. KeyLargo/Intrepid USB
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)
00:0b.0 USB controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family)
 USB2 EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA C
ontroller [AHCI mode] (rev 02)
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ sudo apt install traceroute
[sudo] password for olvildo:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
traceroute is already the newest version (1:2.1.2-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ traceroute google.com
google.com: Temporary failure in name resolution
Cannot handle "host" cmdline arg `google.com' on position 1 (argc 1)
```

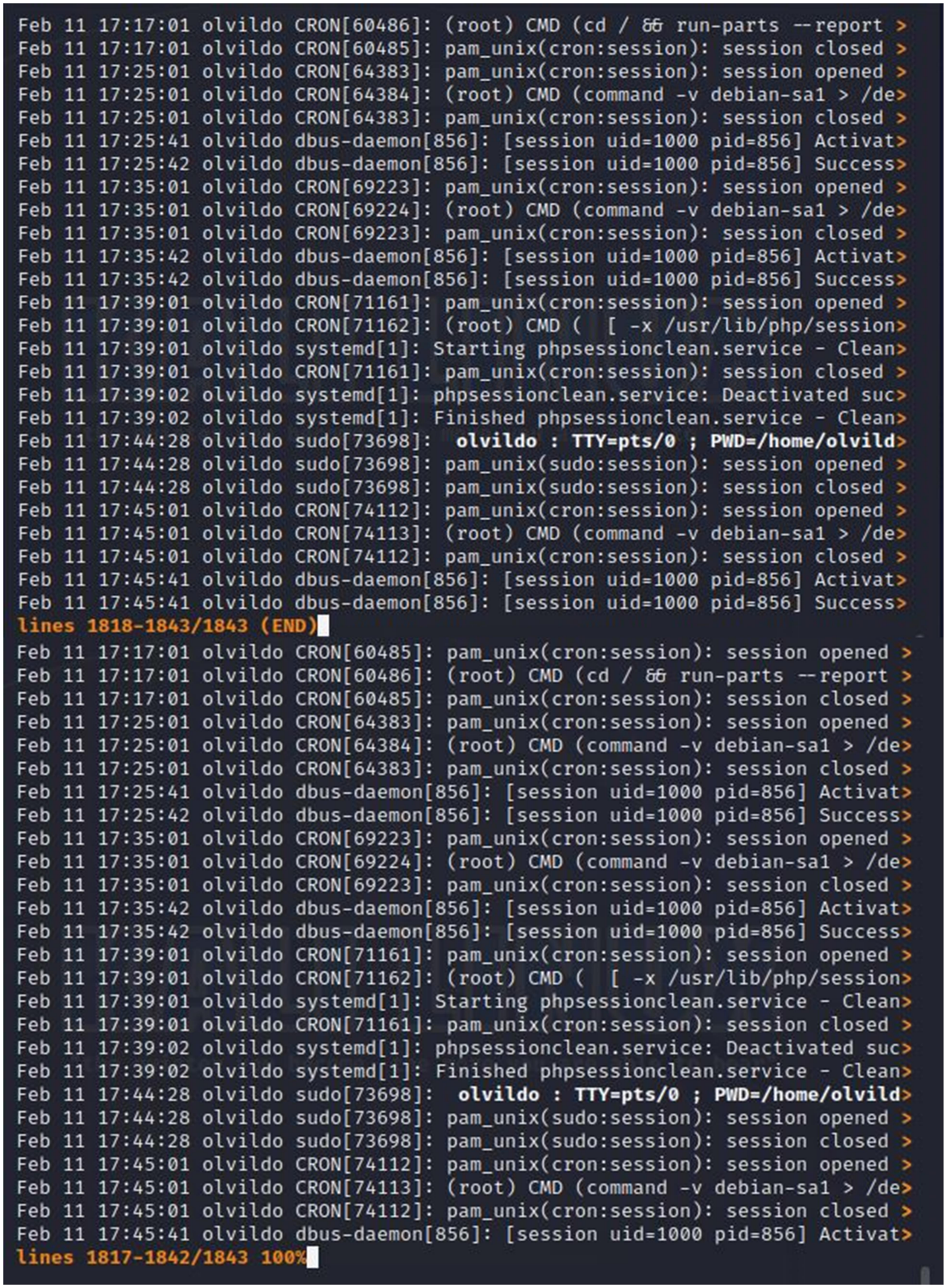
```
┌──(olvildo㉿olvildo)-[~]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ ss -tuln
Netid State  Recv-Q  Send-Q   Local Address:Port   Peer Address:Port Process
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ journalctl
Feb 11 15:13:03 olvildo kernel: Linux version 6.3.0-kali1-amd64 (devel@kali.>
Feb 11 15:13:03 olvildo kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.3.0>
Feb 11 15:13:03 olvildo kernel: x86/fpu: x87 FPU will use FXSAVE
Feb 11 15:13:03 olvildo kernel: signal: max sigframe size: 1440
Feb 11 15:13:03 olvildo kernel: BIOS-provided physical RAM map:
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x000000000009fc00-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x000000007fff0000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000fec00000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000fee00000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000fffc0000-0x0000000>
Feb 11 15:13:03 olvildo kernel: NX (Execute Disable) protection: active
Feb 11 15:13:03 olvildo kernel: SMBIOS 2.5 present.
Feb 11 15:13:03 olvildo kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIO>
Feb 11 15:13:03 olvildo kernel: Hypervisor detected: KVM
Feb 11 15:13:03 olvildo kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 11 15:13:03 olvildo kernel: kvm-clock: using sched offset of 84931056009>
Feb 11 15:13:03 olvildo kernel: clocksource: kvm-clock: mask: 0xffffffffffff>
Feb 11 15:13:03 olvildo kernel: tsc: Detected 2166.666 MHz processor
Feb 11 15:13:03 olvildo kernel: e820: update [mem 0x00000000-0x00000fff] usa>
Feb 11 15:13:03 olvildo kernel: e820: remove [mem 0x000a0000-0x000fffff] usa>
Feb 11 15:13:03 olvildo kernel: last_pfn = 0x7fff0 max_arch_pfn = 0x400000000
```

```
Feb 11 15:13:03 olvildo kernel: pcpu-alloc: [0] 0
Feb 11 15:13:03 olvildo kernel: kvm-guest: PV spinlocks disabled, single CPU
Feb 11 15:13:03 olvildo kernel: Fallback order for Node 0: 0
Feb 11 15:13:03 olvildo kernel: Built 1 zonelists, mobility grouping on.  To>
Feb 11 15:13:03 olvildo kernel: Policy zone: DMA32
Feb 11 15:13:03 olvildo kernel: Kernel command line: BOOT_IMAGE=/boot/vmlinu>
Feb 11 15:13:03 olvildo kernel: Unknown kernel command line parameters "spla>
Feb 11 15:13:03 olvildo kernel: random: crng init done
Feb 11 15:13:03 olvildo kernel: Dentry cache hash table entries: 262144 (ord>
Feb 11 15:13:03 olvildo kernel: Inode-cache hash table entries: 131072 (orde>
Feb 11 15:13:03 olvildo kernel: mem auto-init: stack:all(zero), heap alloc:o>
Feb 11 15:13:03 olvildo kernel: Memory: 260860K/2096696K available (14336K k>
Feb 11 15:13:03 olvildo kernel: SLUB: HWalign=64, Order=0-3, MinObjects=0, C>
Feb 11 15:13:03 olvildo kernel: Kernel/User page tables isolation: enabled
Feb 11 15:13:03 olvildo kernel: ftrace: allocating 41014 entries in 161 pages
Feb 11 15:13:03 olvildo kernel: ftrace: allocated 161 pages with 3 groups
Feb 11 15:13:03 olvildo kernel: Dynamic Preempt: voluntary
Feb 11 15:13:03 olvildo kernel: rcu: Preemptible hierarchical RCU implementa>
Feb 11 15:13:03 olvildo kernel: rcu:         RCU restricting CPUs from NR_CP>
Feb 11 15:13:03 olvildo kernel:         Trampoline variant of Tasks RCU enab>
Feb 11 15:13:03 olvildo kernel:         Rude variant of Tasks RCU enabled.
Feb 11 15:13:03 olvildo kernel:         Tracing variant of Tasks RCU enabled.
Feb 11 15:13:03 olvildo kernel: rcu: RCU calculated value of scheduler-enlis>
Feb 11 15:13:03 olvildo kernel: rcu: Adjusting geometry for rcu_fanout_leaf=>
Feb 11 15:13:03 olvildo kernel: NR_IRQS: 524544, nr_irqs: 256, preallocated >
Feb 11 15:13:03 olvildo kernel: rcu: srcu_init: Setting srcu_struct sizes ba>
Feb 11 15:13:03 olvildo kernel: Console: colour VGA+ 80×25
Feb 11 15:13:03 olvildo kernel: Spectre V2 : Spectre v2 / SpectreRSB : Filli>
Feb 11 15:13:03 olvildo kernel: RETBleed: WARNING: Spectre v2 mitigation lea>
Feb 11 15:13:03 olvildo kernel: RETBleed: Vulnerable
Feb 11 15:13:03 olvildo kernel: MDS: Vulnerable: Clear CPU buffers attempted>
Feb 11 15:13:03 olvildo kernel: MMIO Stale Data: Unknown: No mitigations
Feb 11 15:13:03 olvildo kernel: Freeing SMP alternatives memory: 36K
Feb 11 15:13:03 olvildo kernel: APIC calibration not consistent with PM-Time>
Feb 11 15:13:03 olvildo kernel: APIC delta adjusted to PM-Timer: 6463798 (70>
Feb 11 15:13:03 olvildo kernel: smpboot: CPU0: Intel(R) Celeron(R) CPU  N284>
Feb 11 15:13:03 olvildo kernel: cblist_init_generic: Setting adjustable numb>
Feb 11 15:13:03 olvildo kernel: cblist_init_generic: Setting shift to 0 and >
Feb 11 15:13:03 olvildo kernel: cblist_init_generic: Setting shift to 0 and >
Feb 11 15:13:03 olvildo kernel: cblist_init_generic: Setting shift to 0 and >
Feb 11 15:13:03 olvildo kernel: Performance Events: unsupported p6 CPU model>
Feb 11 15:13:03 olvildo kernel: rcu: Hierarchical SRCU implementation.
Feb 11 15:13:03 olvildo kernel: rcu:         Max phase no-delay instances is>
Feb 11 15:13:03 olvildo kernel: NMI watchdog: Perf NMI watchdog permanently >
Feb 11 15:13:03 olvildo kernel: smp: Bringing up secondary CPUs ...
Feb 11 15:13:03 olvildo kernel: smp: Brought up 1 node, 1 CPU
Feb 11 15:13:03 olvildo kernel: smpboot: Max logical packages: 1
Feb 11 15:13:03 olvildo kernel: smpboot: Total of 1 processors activated (43>
Feb 11 15:13:03 olvildo kernel: node 0 deferred pages initialised in 12ms
Feb 11 15:13:03 olvildo kernel: devtmpfs: initialized
Feb 11 15:13:03 olvildo kernel: x86/mm: Memory block size: 128MB
Feb 11 15:13:03 olvildo kernel: clocksource: jiffies: mask: 0×ffffffff max_c>
Feb 11 15:13:03 olvildo kernel: clocksource: jiffies: mask: 0×ffffffff max_c>
Feb 11 15:13:03 olvildo kernel: futex hash table entries: 256 (order: 2, 163>
```

```
Feb 11 15:13:03 olvildo kernel: smp: Brought up 1 node, 1 CPU
Feb 11 15:13:03 olvildo kernel: smpboot: Max logical packages: 1
Feb 11 15:13:03 olvildo kernel: smpboot: Total of 1 processors activated (43>
Feb 11 15:13:03 olvildo kernel: node 0 deferred pages initialised in 12ms
Feb 11 15:13:03 olvildo kernel: devtmpfs: initialized
Feb 11 15:13:03 olvildo kernel: x86/mm: Memory block size: 128MB
Feb 11 15:13:03 olvildo kernel: clocksource: jiffies: mask: 0×ffffffff max_c>
Feb 11 15:13:03 olvildo kernel: futex hash table entries: 256 (order: 2, 163>
Feb 11 15:13:03 olvildo kernel: pinctrl core: initialized pinctrl subsystem
Feb 11 15:13:03 olvildo kernel: NET: Registered PF_NETLINK/PF_ROUTE protocol>
Feb 11 15:13:03 olvildo kernel: DMA: preallocated 256 KiB GFP_KERNEL pool fo>
Feb 11 15:13:03 olvildo kernel: DMA: preallocated 256 KiB GFP_KERNEL|GFP_DMA>
Feb 11 15:13:03 olvildo kernel: DMA: preallocated 256 KiB GFP_KERNEL|GFP_DMA>
Feb 11 15:13:03 olvildo kernel: audit: initializing netlink subsys (disabled)
Feb 11 15:13:03 olvildo kernel: thermal_sys: Registered thermal governor 'fa>
Feb 11 15:13:03 olvildo kernel: thermal_sys: Registered thermal governor 'ba>
Feb 11 15:13:03 olvildo kernel: thermal_sys: Registered thermal governor 'st>
Feb 11 15:13:03 olvildo kernel: thermal_sys: Registered thermal governor 'us>
Feb 11 15:13:03 olvildo kernel: thermal_sys: Registered thermal governor 'po>
Feb 11 15:13:03 olvildo kernel: cpuidle: using governor ladder
Feb 11 15:13:03 olvildo kernel: cpuidle: using governor menu
Feb 11 15:13:03 olvildo kernel: acpiphp: ACPI Hot Plug PCI Controller Driver>
Feb 11 15:13:03 olvildo kernel: PCI: Using configuration type 1 for base acc>
Feb 11 15:13:03 olvildo kernel: kprobes: kprobe jump-optimization is enabled>
Feb 11 15:13:03 olvildo kernel: audit: type=2000 audit(1739313259.603:1): st>
Feb 11 15:13:03 olvildo kernel: HugeTLB: registered 2.00 MiB page size, pre->
Feb 11 15:13:03 olvildo kernel: HugeTLB: 28 KiB vmemmap can be freed for a 2>
Feb 11 15:13:04 olvildo kernel: evm: security.capability
Feb 11 15:13:04 olvildo kernel: evm: HMAC attrs: 0×1
Feb 11 15:13:04 olvildo kernel: Freeing unused decrypted memory: 2036K
Feb 11 15:13:04 olvildo kernel: Freeing unused kernel image (initmem) memory>
Feb 11 15:13:04 olvildo kernel: Write protecting the kernel read-only data: >
Feb 11 15:13:04 olvildo kernel: Freeing unused kernel image (rodata/data gap>
Feb 11 15:13:04 olvildo kernel: x86/mm: Checked W+X mappings: passed, no W+X>
Feb 11 15:13:04 olvildo kernel: x86/mm: Checking user space page tables
Feb 11 15:13:04 olvildo kernel: x86/mm: Checked W+X mappings: passed, no W+X>
Feb 11 15:13:04 olvildo kernel: Run /init as init process
Feb 11 15:13:04 olvildo kernel:   with arguments:
Feb 11 15:13:04 olvildo kernel:     /init
Feb 11 15:13:04 olvildo kernel:     splash
Feb 11 15:13:04 olvildo kernel:   with environment:
Feb 11 15:13:04 olvildo kernel:     HOME=/
Feb 11 15:13:04 olvildo kernel:     TERM=linux
Feb 11 15:13:04 olvildo kernel:     BOOT_IMAGE=/boot/vmlinuz-6.3.0-kali1-amd>
Feb 11 15:13:04 olvildo kernel: input: Power Button as /devices/LNXSYSTM:00/>
Feb 11 15:13:04 olvildo kernel: ACPI: video: Video Device [GFX0] (multi-head>
Feb 11 15:13:04 olvildo kernel: ACPI: button: Power Button [PWRF]
Feb 11 15:13:04 olvildo kernel: input: Sleep Button as /devices/LNXSYSTM:00/>
Feb 11 15:13:04 olvildo kernel: ACPI: button: Sleep Button [SLPF]
Feb 11 15:13:04 olvildo kernel: input: Video Bus as /devices/LNXSYSTM:00/LNX>
Feb 11 15:13:04 olvildo kernel: e1000: Intel(R) PRO/1000 Network Driver
Feb 11 15:13:04 olvildo kernel: e1000: Copyright (c) 1999-2006 Intel Corpora>
Feb 11 15:13:04 olvildo kernel: ACPI: battery: Slot [BAT0] (battery present)
lines 329-354
```


Feb 11 17:17:01 olvildo CRON[60486]: (root) CMD (cd / && run-parts --report >
Feb 11 17:17:01 olvildo CRON[60485]: pam_unix(cron:session): session closed >
Feb 11 17:25:01 olvildo CRON[64383]: pam_unix(cron:session): session opened >
Feb 11 17:25:01 olvildo CRON[64384]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:25:01 olvildo CRON[64383]: pam_unix(cron:session): session closed >
Feb 11 17:25:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
Feb 11 17:25:42 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Success>
Feb 11 17:35:01 olvildo CRON[69223]: pam_unix(cron:session): session opened >
Feb 11 17:35:01 olvildo CRON[69224]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:35:01 olvildo CRON[69223]: pam_unix(cron:session): session closed >
Feb 11 17:35:42 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
Feb 11 17:35:42 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Success>
Feb 11 17:39:01 olvildo CRON[71161]: pam_unix(cron:session): session opened >
Feb 11 17:39:01 olvildo CRON[71162]: (root) CMD ([-x /usr/lib/php/session>
Feb 11 17:39:01 olvildo systemd[1]: Starting phpsessionclean.service - Clean>
Feb 11 17:39:01 olvildo CRON[71161]: pam_unix(cron:session): session closed >
Feb 11 17:39:02 olvildo systemd[1]: phpsessionclean.service: Deactivated suc>
Feb 11 17:39:02 olvildo systemd[1]: Finished phpsessionclean.service - Clean>
Feb 11 17:44:28 olvildo sudo[73698]: olvildo : TTY=pts/0 ; PWD=/home/olvild>
Feb 11 17:44:28 olvildo sudo[73698]: pam_unix(sudo:session): session opened >
Feb 11 17:44:28 olvildo sudo[73698]: pam_unix(sudo:session): session closed >
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session opened >
Feb 11 17:45:01 olvildo CRON[74113]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session closed >
Feb 11 17:45:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
Feb 11 17:45:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Success>
lines 1818-1843/1843 (END)
Feb 11 17:17:01 olvildo CRON[60485]: pam_unix(cron:session): session opened >
Feb 11 17:17:01 olvildo CRON[60486]: (root) CMD (cd / && run-parts --report >
Feb 11 17:17:01 olvildo CRON[60485]: pam_unix(cron:session): session closed >
Feb 11 17:25:01 olvildo CRON[64383]: pam_unix(cron:session): session opened >
Feb 11 17:25:01 olvildo CRON[64384]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:25:01 olvildo CRON[64383]: pam_unix(cron:session): session closed >
Feb 11 17:25:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
Feb 11 17:25:42 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Success>
Feb 11 17:35:01 olvildo CRON[69223]: pam_unix(cron:session): session opened >
Feb 11 17:35:01 olvildo CRON[69224]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:35:01 olvildo CRON[69223]: pam_unix(cron:session): session closed >
Feb 11 17:35:42 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
Feb 11 17:35:42 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Success>
Feb 11 17:39:01 olvildo CRON[71161]: pam_unix(cron:session): session opened >
Feb 11 17:39:01 olvildo CRON[71162]: (root) CMD ([-x /usr/lib/php/session>
Feb 11 17:39:01 olvildo systemd[1]: Starting phpsessionclean.service - Clean>
Feb 11 17:39:01 olvildo CRON[71161]: pam_unix(cron:session): session closed >
Feb 11 17:39:02 olvildo systemd[1]: phpsessionclean.service: Deactivated suc>
Feb 11 17:39:02 olvildo systemd[1]: Finished phpsessionclean.service - Clean>
Feb 11 17:44:28 olvildo sudo[73698]: olvildo : TTY=pts/0 ; PWD=/home/olvild>
Feb 11 17:44:28 olvildo sudo[73698]: pam_unix(sudo:session): session opened >
Feb 11 17:44:28 olvildo sudo[73698]: pam_unix(sudo:session): session closed >
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session opened >
Feb 11 17:45:01 olvildo CRON[74113]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session closed >
Feb 11 17:45:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
lines 1817-1842/1843 100%

```
┌──(olvildo㉿olvildo)-[~]
└─$ journalctl -f
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session opened f
or user root(uid=0) by (uid=0)
Feb 11 17:45:01 olvildo CRON[74113]: (root) CMD (command -v debian-sa1 > /dev
/null && debian-sa1 1 1)
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session closed f
or user root
Feb 11 17:45:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activati
ng service name='org.xfce.Xfconf' requested by ':1.23' (uid=1000 pid=1061 com
m="xfce4-panel")
Feb 11 17:45:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Successf
ully activated service 'org.xfce.Xfconf'
Feb 11 17:55:01 olvildo CRON[78953]: pam_unix(cron:session): session opened f
or user root(uid=0) by (uid=0)
Feb 11 17:55:01 olvildo CRON[78954]: (root) CMD (command -v debian-sa1 > /dev
/null && debian-sa1 1 1)
Feb 11 17:55:01 olvildo CRON[78953]: pam_unix(cron:session): session closed f
or user root
Feb 11 17:55:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activati
ng service name='org.xfce.Xfconf' requested by ':1.23' (uid=1000 pid=1061 com
m="xfce4-panel")
Feb 11 17:55:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Successf
ully activated service 'org.xfce.Xfconf'
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ journalctl -b
Feb 11 15:13:03 olvildo kernel: Linux version 6.3.0-kali1-amd64 (devel@kali.>
Feb 11 15:13:03 olvildo kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.3.0>
Feb 11 15:13:03 olvildo kernel: x86/fpu: x87 FPU will use FXSAVE
Feb 11 15:13:03 olvildo kernel: signal: max sigframe size: 1440
Feb 11 15:13:03 olvildo kernel: BIOS-provided physical RAM map:
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x000000000009fc00-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x000000007fff0000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000fec00000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000fee00000-0x0000000>
Feb 11 15:13:03 olvildo kernel: BIOS-e820: [mem 0x00000000fffc0000-0x0000000>
Feb 11 15:13:03 olvildo kernel: NX (Execute Disable) protection: active
Feb 11 15:13:03 olvildo kernel: SMBIOS 2.5 present.
Feb 11 15:13:03 olvildo kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIO>
Feb 11 15:13:03 olvildo kernel: Hypervisor detected: KVM
Feb 11 15:13:03 olvildo kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 11 15:13:03 olvildo kernel: kvm-clock: using sched offset of 84931056009>
Feb 11 15:13:03 olvildo kernel: clocksource: kvm-clock: mask: 0xffffffffffff>
Feb 11 15:13:03 olvildo kernel: tsc: Detected 2166.666 MHz processor
Feb 11 15:13:03 olvildo kernel: e820: update [mem 0x00000000-0x00000fff] usa>
Feb 11 15:13:03 olvildo kernel: e820: remove [mem 0x000a0000-0x000fffff] usa>
Feb 11 15:13:03 olvildo kernel: last_pfn = 0x7fff0 max_arch_pfn = 0x400000000
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ journalctl -n 10
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session opened >
Feb 11 17:45:01 olvildo CRON[74113]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:45:01 olvildo CRON[74112]: pam_unix(cron:session): session closed >
Feb 11 17:45:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
Feb 11 17:45:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Success>
Feb 11 17:55:01 olvildo CRON[78953]: pam_unix(cron:session): session opened >
Feb 11 17:55:01 olvildo CRON[78954]: (root) CMD (command -v debian-sa1 > /de>
Feb 11 17:55:01 olvildo CRON[78953]: pam_unix(cron:session): session closed >
Feb 11 17:55:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Activat>
Feb 11 17:55:41 olvildo dbus-daemon[856]: [session uid=1000 pid=856] Success>
lines 1-10/10 (END)
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ date
Tue Feb 11 18:00:18 EST 2025
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ timedatectl
               Local time: Tue 2025-02-11 18:00:34 EST
           Universal time: Tue 2025-02-11 23:00:34 UTC
                 RTC time: Tue 2025-02-11 23:00:33
                Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

```
┌──(olvildo㉿olvildo)-[~]
└─$ hostnamectl
 Static hostname: olvildo
       Icon name: computer-vm
         Chassis: vm
      Machine ID: c56125d0cdea4551af82e2c105b80311
         Boot ID: b8ec873a089d47eb8cd9c16bb99e2626
  Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 6.3.0-kali1-amd64
    Architecture: x86-64
 Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox
Firmware Version: VirtualBox
   Firmware Date: Fri 2006-12-01
    Firmware Age: 18y 2month 1w 5d
```